



## **AWARD ATTACHMENTS**

CENTER FOR INTERNET SECURITY, INC.

23CISMSI00003-01-00

---

1. Award Letter
2. Cooperative Agreement Terms and Conditions
3. FY23 DHS Standard Terms and Conditions
4. Appendix A
5. Appendix B



Homeland  
Security

September 27, 2023

[REDACTED]  
Center for Internet Security  
31 Tech Valley Drive  
East Greenbush, NY 12061-4134

**Re: Award Number: 23CISMSI00003-01-00**  
*State, Local, Tribal and Territorial (SLTT) Security Operations Center (SOC) | Information Sharing and Analysis Center (ISAC)*

Dear [REDACTED]

Congratulations on being selected as the 2023 recipient of the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency: State, Local, Tribal and Territorial Security Operations Center | Information Sharing and Analysis Center Cooperative Agreement. Your application was awarded in the amount of **\$61,432,857** for the period of September 30, 2023, to September 29, 2024. This amount includes a total of \$43,003,000 in FY23 Base Funding and a total of \$18,429,857 in Recipient Cost Share. Please note that a portion of the funding is restricted per the award terms and conditions.

This award is made subject to the terms and conditions of the enclosed Assistance Agreement. If any additional assistance is required, please have your staff contact [REDACTED] Project Officer, at [REDACTED] on technical/programmatic matters, or [REDACTED] Grants Officer at [REDACTED] on administrative matters.

Congratulations again! We look forward to partnering with you on this important project.

[REDACTED]  
Grants and Financial Assistance Division  
Office of Procurement Operations  
Department of Homeland Security

## **COOPERATIVE AGREEMENT TERMS AND CONDITIONS**

Program: State, Local, Tribal, and Territorial (SLTT) Security Operations Center (SOC) | Information Sharing and Analysis Center (ISAC)

Recipient: Center for Internet Security

Federal Award No: 23CISMSI00003

Amendment: 1

### **ARTICLE I. DHS STANDARD TERMS AND CONDITIONS**

The terms and conditions set forth in the Fiscal Year 2023 Department of Homeland Security Standard Terms and Conditions, v. 2 (Nov. 29, 2022) are incorporated by reference into the Federal Award. These are available at [www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions](https://www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions).

### **ARTICLE II. GENERAL ADMINISTRATIVE TERMS AND CONDITIONS**

#### **A. AWARD SPECIFIC TERMS AND CONDITIONS**

##### **1. Notice of Funding Opportunity**

All instructions, guidance, performance goals, limitations, scope of work, and other conditions set forth in the Notice of Funding Opportunity for the FY 2023 State, Local, Tribal, and Territorial Security Operations Center Information Sharing and Analysis Center are incorporated by reference into the Federal Award. The Notice of Funding Opportunity is available at [www.grants.gov](https://www.grants.gov).

##### **2. Applicability and Post Award Changes**

The terms and conditions set forth in this document and elsewhere in the award package will apply to the initial and all future budget periods for the Federal Award. As part of approving an additional budget period and awarding additional funding for the Federal Award, DHS/CISA may revise the terms and conditions and/or other parts of the award package. DHS/CISA will notify the Recipient in writing of the change and provide an updated award package document to the Recipient for review.

Separate and distinct from making changes when approving an additional budget period, DHS/CISA may revise terms and conditions and other parts of the award package if it determines that there was an error in the award package or otherwise determines that an administrative change must be made to the award package. DHS/CISA will notify the Recipient in writing of the change and provide an updated award package document to the Recipient for review. Once notification occurs, any subsequent request for funds will indicate Recipient acceptance of the changes to the Federal Award.

##### **3. Award Restrictions**

Of the total funds Awarded, \$1,000,000 is restricted from use. The Recipient must use the Program Management or the Project and Portfolio Management categories to incur expenses for planning



activities related to the following restricted funds. The restricted funds may only be used once approved by CISA Program Officer (PO).

To request use of restricted funds, the Recipient will submit an email to CISA PO requesting the release of the funds, with requested funding amount and description of use of funds. In addition, the Recipient will provide the information outlined below for each program or activity. No restricted funds will be released until CISA PO notifies responsible Grants Office of approval. Once restricted funds are released, an amendment or subsequent documentation will be provided to the Recipient by the DHS Grants Office. If the request is not approved, CISA PO will send Recipient an email outlining the reason for denial.

- a. Annual Multi-State Information Sharing & Analysis Center (ISAC) Membership Meeting funds in the amount of \$1,000,000 are restricted until CISA PO approval has been authorized. To request release of funds, the Recipient must provide the following data prior to committing resources:
  - i. Finalized meeting planning package
  - ii. Choice and cost of venue and services

#### 4. Project Milestones, Deliverables, and Timelines

- a. Changes to the Details, Objectives, Performance Metrics, and timelines outlined in Appendix A are subject to CISA PO review and prior approval. Any changes initiated or proposed by the Recipient should be submitted via email to the CISA PO for review and approval along with a programmatic justification and budget impact statement.
- b. The Recipient-submitted Program Management Plan (PMP) establishes technical milestones and deliverables. If the Recipient fails to achieve two or more technical milestones and deliverables, CISA PO may request modifications to the PMP. In the alternative, CISA PO may deem the Recipient's failure to achieve these technical milestones and deliverables to be material noncompliance with the terms and conditions of this Award and take action to require a Corrective Action Plan, reduce or restrict funding, or suspend or terminate the Award.

#### 5. Monthly Financial Activity-Based Costing (ABC) Report

- a. CISA PO will provide a formatted template for an activity-based costing model that identifies program activities. The Recipient will then assign the cost of each activity with resources to all program services and according to the actual consumption by each. CISA PO reserves the right to amend the format as necessary. Activity Reports will be delineated by fixed/variable cost drivers that define logical elements of capability. Report will include, but not be limited to: Funding Burn Rates, Partner-paid cost share, Budget Forecast, Estimate At Completion (EAC), Budget vs EAC variance. ABC Reports shall be submitted along with IPR materials each month. Reports shall be emailed to the CISA PO at [REDACTED] and uploaded to the GrantSolutions system, using the Grant Note feature. Guidance is found here: <https://www.grantsolutions.gov/support/granteeUsers.html>

#### 6. Monthly In-Progress Review (IPR) and Quarterly Program Management Review (PMR)

- a. In addition to what is stated in Appendix A and Appendix B, slides for the monthly IPR must contain accurate and up-to-date information (including but not limited to financial information, operational data, and program status) and be sent to CISA PO at [REDACTED] no later than the 15th of the month and reflect the previous month's data. Additionally, a knowledgeable representative from Recipient shall be on the IPR calls to answer questions regarding the presented slides.
- b. In addition to what is stated in Appendix A and Appendix B, slides for the quarterly PMR must contain accurate and up-to-date information (including but not limited to financial information, operational data,

and program status) and be sent to CISA PO at [REDACTED] no later than the 15th of the month and reflect the previous quarter's data. Additionally, a knowledgeable representative from Recipient shall be on the PMR calls to answer questions regarding the presented slides.

## **B. DHS PROGRAMMATIC INVOLVEMENT**

The funding instrument used for this program will be the cooperative agreement, an assistance mechanism in which substantial CISA Program Office (PO) involvement is anticipated during the period of performance. Under the cooperative agreement, CISA supports and stimulates the Recipient's activities by involvement in, and otherwise working jointly with the Recipient in a partnership role; it is not to assume direction, prime responsibility, or a dominant role in activities. Consistent with this premise, the dominant role and prime responsibility resides with the Recipient for the program.

- a. To facilitate appropriate involvement, during the period of this cooperative agreement, CISA PO and the Recipient will be in contact monthly and more frequently as appropriate to ensure successful execution. Specific tasks and activities that may be shared between the Recipient and CISA PO include but are not limited to:
  - i. Providing strategic/tactical guidance and feedback in furtherance of the goals and objectives of the award.
  - ii. Providing access to key staff groups and other varied technical and programmatic resources, offering subject matter expertise, and liaising with stakeholders.
  - iii. Reviewing deliverables before dissemination.
  - iv. Ending an activity if performance specifications are not met.
  - v. Exchanging bi-directional cyber threat information and building TTP (Tactics, Techniques and Procedures) context in furtherance of the objectives to enable a collective defense model.
  - vi. Exchanging unattributed and attributed cyber threat landscape information.
- b. CISA PO will be responsible for substantial involvement to include, but are not limited to the following:
  - i. CISA PO will provide substantial programmatic involvement during the performance period. Oversight services at the highest level are to keep CISA leadership apprised of the program status and to identify and quickly mitigate any threats to on-time and on-budget completion.
  - ii. Substantial federal involvement includes administrative activities such as monitoring and reviewing project phases. CISA PO will not direct or recommend that the Recipient enter a contract with a particular entity.
  - iii. CISA will provide promotional support of the SLTT SOC|ISAC program and its services with the goal of increasing SLTT trusted community interest and fulfilling the vision of an interconnected cyber ecosystem.
  - iv. CISA PO will provide administrative assistance related to security clearances to complete the approved scope of work.
  - v. CISA will allocate sufficient office space and communications, IT systems, telephones, and administrative supplies at CISA for cyber liaison officers to sit "side-by-side" with federal colleagues to facilitate effective unity of effort in the situational awareness assessment of the SLTT community that is used to prepare the national cyber assessment.
  - vi. CISA will provide reception and integration of the LNO team into CISA by identifying a single CISA staff member who is assigned the responsibility to assimilate the LNOs and provide the access they need to perform their functions.
  - vii. CISA will provide Homeland Security Information Network (HSIN) platform resources for trusted sharing of Sensitive but Unclassified Information with the SLTT community.

- viii. CISA will assist in the establishment of Federal interagency partnerships, collaboration and cooperation that may be necessary for carrying out the program.
- ix. CISA PO will provide, when appropriate, subject matter experts (SMEs) and other varied technical and programmatic resources to support each component of the program as defined in Appendix A.
- x. CISA PO representatives will attend and participate in meetings initiated by the Recipient, as defined by CISA.
- xi. CISA will assist in the establishment of partnerships, collaboration, and cooperation with Federal, State, local, tribal, or territorial governments, or private entities that may be necessary for carrying out the project.
- xii. CISA and the Recipient (on behalf of the ISACs) will exchange bi-directional cyber threat indicators and information in furtherance of the objectives and priorities delineated in Appendix A to enable a collective defense model.
- xiii. For purposes of maintaining cyber situational awareness of issues that affect reliability and resilience of the SLTT, CISA may exchange unattributed and attributed cyber threat landscape information with the ISACs.
- xiv. CISA will hold equity calls with federal officials and the ISACs on SLTT/Elections victim notification.
- xv. CISA will, as the program support deems necessary, facilitate coordination to address cybersecurity risks and incidents, in the form of email, site visits, teleconferences, workshops, webinars, technical exchanges, sharing cyber threat indicators and vulnerabilities, cyber analytic and awareness products, training opportunities, tabletop exercises, and technical assistance upon request.
- xvi. CISA may halt an activity immediately if detailed performance specifications or requirements are not met.
- xvii. CISA PO may review and approve one stage of work before the Recipient may begin a subsequent stage during the period covered by the Award. For purposes of this item, a "stage" is a significant phase of a project (not individual tasks).
- xviii. CISA PO may be involved in the key Recipient personnel assigned to perform work under the federal Award CISA PO and the Recipient will partner or collaborate in project activities.
- xix. CISA PO may undertake monitoring that permit CISA PO to direct or redirect the work because of interrelationships with another program.
- xx. Substantial and direct operational involvement of or participation by CISA PO in the project is anticipated before the award is made to ensure compliance with such statutory requirements as civil rights, environmental protection, and provisions for the disabled. Such participation would exceed what is normally undertaken to comply with general statutory requirements that are a condition of every award.
- xxi. CISA PO will provide substantial involvement in the form of technical collaboration or participation in carrying out the scope of work, development of outputs, and oversight.
- xxii. CISA PO will provide promotional support of the SLTT SOC|ISAC program and its services with the goal of increasing SLTT trusted community interest and fulfilling the vision of an interconnected cyber ecosystem.
- xxiii. CISA PO will provide, when appropriate, subject matter experts (SMEs) and other varied technical and programmatic resources to support each component of the program as defined in Appendix A.
- xxiv. CISA PO representatives will attend and participate in appropriate meetings initiated by the Recipient.
- xxv. For purposes of maintaining cyber situational awareness of issues that affect reliability and resilience of the SLTT, CISA PO and the Recipient will exchange unattributed and attributed cyber threat landscape information.
- xxvi. CISA PO will make available office space at CISA PO for analysts to sit "side-by-side" with federal colleagues to provide the situational awareness assessment for the SLTT and Elections community that is used to prepare the national cyber assessment.
- xxvii. CISA PO provides a compartment on the HSIN platform for sharing information with the SLTT community and CISA staff populate the site with shared federal cyber awareness products.



CISA will provide substantial technical involvement during the Period of Performance. Multiple offices anticipate providing technical assistance and subject matter expertise support to the Recipient. The Recipient will anticipate receiving information directly from these offices and their and their contractors. The offices include but not limited to: The Office of the Executive Assistant Director for Cybersecurity Division (CSD) and its sub-divisions of Capacity Building, Mission Engineering, Threat Hunting, Vulnerability Management, and Joint Cyber Defense Collaborative (JCDC); as well as other divisions of CISA, including National Risk Management Center (NRMC), Stakeholder Engagement Division (SED), Integrated Operations Division (IOD), Emergency Communications Division (ECD), and Infrastructure Security Division (ISD).

## **B. AMENDMENTS AND REVISIONS**

### **1. Budget Revisions**

- a. Transfers of funds between direct cost categories in the approved budget when such cumulative transfers among those direct cost categories exceed ten percent of the total budget approved in this Award require prior written approval by the CISA PO and DHS Grants Officer.
- b. All requests for budget revisions requiring prior approval under 2 C.F.R. § 200.308 must be submitted to the CISA PO and DHS Grants Officer.
- c. To avoid expenditures on products and services duplicating CISA capabilities or products/services that are already commercially available, the Recipient must obtain the written approval from CISA PO prior to the development of new services delivered to SLTT stakeholders under the Federal Award that are not outlined in the approved budget or are otherwise commercially available. CISA PO reserves the right based on project milestones and/or timelines to require the use of commercially available products/services in order to achieve cost and time efficiencies.
- d. The Recipient is not authorized at any time to transfer amounts budgeted for direct costs to the indirect costs line item or vice versa, without prior written approval of the DHS Grants Officer.

### **2. Extension Request**

- a. The Recipient must submit all requests for extensions to the Period of Performance to the PO and Grants Officer for consideration sixty (60) days before the expiration date of the Period of Performance.
- b. Requests for time extensions to the Period of Performance will be considered but will not be approved automatically and must be supported by adequate justification to be processed. The justification is a written explanation of the reason or reasons for the delay; an outline of remaining resources/funds available to support the extended Period of Performance; and a description of performance measures necessary to complete the project. Without performance and financial status reports current and justification submitted, the PO and Grant Officer will not process extension requests.
- c. DHS/CISA has no obligation to provide additional resources/funding as a result of an extension.

## **C. FINANCIAL REPORTING**

1. Semi-Annual Federal Financial Reports - the Recipient must submit a Federal Financial Report (SF425) to

the DHS/CISA Grants Officer no later than 30 days after the end of the reporting period end date. Reports are due on 4/30 and 10/31. The report must be submitted electronically via [www.GrantSolutions.gov](http://www.GrantSolutions.gov). Please select the FFR submission guidance found here: <https://www.Grantsolutions.gov/support/granteeUsers.html>.

2. Quarterly Federal Financial Reports (Cash Transaction) - the Recipient must submit the Federal Financial Report (SF425) Cash Transaction Report to the Department of Health and Human Services, Payment Management System. Quarterly Cash Transaction reports must be submitted no later than 1/31, 4/30, 7/31, and 10/31.

3. Final Federal Financial Report -the Recipient must submit the final Federal Financial Report (SF425) to the DHS/CISA Grants Officer no later than 120 days after the end of the Period of Performance. The report must be submitted electronically via [www.GrantSolutions.gov](http://www.GrantSolutions.gov). Please select the FFR submission guidance found here: <https://www.Grantsolutions.gov/support/granteeUsers.html>.C.5

#### **D. FUTURE BUDGET PERIODS**

The approval of subsequent budget periods under the Federal Award is contingent on the following as determined by DHS/CISA:

1. Acceptable performance under the Federal Award;
2. Program authority;
3. Compliance with the terms and conditions of the Federal Award;
4. If applicable, acceptance and approval of each non-competing continuation application;
5. Availability of appropriated funds; and
6. Determination that continued funding is in the best interests of the federal government.

#### **E. PERFORMANCE REPORTS**

1. Quarterly Performance Reports - the Recipient must submit performance reports to the DHS/CISA Grants Officer no later than 30 days after the end of the reporting period end date. Reports are due on the following dates: 01/31, 04/30, 07/31 and 10/31. The report must be submitted via GrantSolutions using the Help/Support Reference entitled, Grant Recipient Process: [Performance Progress Reporting](#).
2. Performance reports must provide information on the overall progress by quarter and by fiscal year. These reports must include:
  - i. A summary that clearly differentiates between activities completed under the SLTT SOC|ISAC cooperative agreement and related activities completed with other sources of leveraged funding.
  - ii. Performance Metric Reporting as outlined in Appendix A Task 10.
  - iii. A summary and status of approved activities performed during the reporting period; a summary of the performance outputs/outcomes achieved during the reporting period; and a description of problems encountered during the reporting period that may affect the project schedule.
  - iv. A comparison of actual accomplishments with the goals and objectives established for

- the period in the DHS/CISA-approved workplan.
  - v. Difficulties encountered and reasons why established objectives were not met, if applicable.
  - vi. An update on project schedules and milestones, including an explanation of any discrepancies from the DHS/CISA-approved workplan.
  - vii. A discussion of expenditures and financial status for each workplan task, along with a comparison of the percentage of the project completed to the project schedule and an explanation of significant discrepancies shall be included in the report.
  - viii. A budget recap summary table with the following information: current approved project budget; DHS/CISA funds drawn down during the reporting period; costs drawn down to date (cumulative expenditures); program income generated and used (if applicable); and total remaining funds.
  - ix. Other pertinent information including, when appropriate, any discrepancies in the budget from the DHS/CISA-approved workplan, analysis and explanation of cost overruns or high unit costs.
  - x. For the quarterly performance reports, provide a high-level comparison between the last quarterly report and the current reporting period.
  - xi. At the end of the fourth quarter provide both a fourth quarter performance report and an Annual Summary Performance Report.
3. If the performance report contains any information that is deemed proprietary, the Recipient will denote the beginning and ending of such information with asterisks (\*\*\*\*\*).
  4. In accordance with 2 C.F.R. § 200.329(e)(1), the Recipient will inform DHS/CISA via email, as soon as problems, delays, or adverse conditions become known which will impair the ability to meet the outcomes specified in the DHS/CISA-approved workplan.
  5. Final Performance Report - the Recipient must submit the Final Performance Report to the DHS/CISA Grants Officer no later than 120 days after the expiration of the Period of Performance. The report must be submitted via GrantSolutions using the Help/Support Reference entitled, Grant Recipient Process: Performance Progress Reporting.

## **F. EQUIPMENT**

1. Title to equipment acquired by the Recipient under this Award will vest in the Recipient, subject to the conditions pertaining to equipment in the 2 C.F.R. Part 200.
2. The Recipient will submit a master list of all CISA funded equipment within 90 days of Award. Master list will include all required inventory information listed in sub paragraph 4.
3. The Recipient must obtain prior written approval from DHS/CISA before purchasing equipment as detailed in 2 C.F.R. § 200.439.
4. The Recipient must submit a quarterly equipment report broken down into the following categories: SLTT/Elections (equipment used for both SLLT and election infrastructure services), Elections-specific (equipment solely used for election infrastructure) and Management (equipment used by Recipient to manage the cooperative agreement). The report will contain a description of the property; manufacturer model number, serial number, or other identification number; the source of property; name on title; acquisition date; and cost of the unit; the address of use; operational condition of the property; and, disposition data, if applicable. Disposed equipment is to remain on the inventory report. This report will be maintained and due with the Quarterly Performance Reports, and must be submitted electronically via [www.GrantSolutions.gov](http://www.GrantSolutions.gov) using the Grant Note feature and guidance



found here: <https://www.grantsolutions.gov/support/granteeUsers.html>.

5. When original or replacement equipment acquired under the Award is no longer needed for the original project or program or for other activities currently or previously supported by a federal awarding agency, the Recipient entity must obtain written disposition instructions from DHS/CISA. DHS/CISA may direct that the Recipient transfer title to the property to the federal government or to a third party.

## **G. PAYMENT**

The Recipient will be paid in advance using the U.S. Department of Health and Human Services/Payment Management System, provided it maintains or demonstrates the willingness and ability to maintain procedures to minimize the time elapsing between the transfer of the funds from DHS/CISA and expenditure disbursement by the Recipient. When these requirements are not met, the Recipient will be required to be on a reimbursement for costs incurred method.

Any overpayment of funds must be coordinated with the U.S. Department of Health and Human Services/Payment Management System.

## **ARTICLE III. GENERAL TERMS AND CONDITIONS**

### **A. ACCESS TO RECORDS**

1. The Recipient and subrecipients must retain financial records, supporting documents, statistical records, and all other records pertinent to the Award or subaward for a period of three years from the date of submission of the final expenditure report pursuant to 2 C.F.R. § 200.334. There are various **exceptions** to the aforementioned record retention requirement set forth in 2 C.F.R. § 200.334,
2. DHS/CISA, the Inspector General, Comptroller General of the United States, or any of their duly authorized representatives, have the right of access to any documents, papers, or other records of the Recipient and subrecipients that are pertinent to this Award, in order to make audits, examinations, excerpts, and transcripts of such documents. This right also includes timely and reasonable access to Recipient and subrecipient personnel for the purpose of interview and discussion related to such documents. The rights of access in this Award term are not limited to the required retention period but last as long as the records are retained.
3. The Recipient will include in any subaward the requirements of this Award term (Access to Records).

### **B. COMPLIANCE ASSURANCE PROGRAM OFFICE TERMS AND CONDITIONS**

The Compliance Assurance Program Office (CAPO) is comprised of the DHS Treaty Compliance Office (TCO), Export Control Group (ECG), and the DHS Regulatory Compliance Office (RCO). The Compliance Assurance Program Manager (CAPM) is the DHS official responsible for overseeing CAPO and implementing procedures to ensure that the Recipient and any Recipient institutions/collaborators under this Award comply with international treaties, federal regulations, and DHS policies for Arms Control Agreements, Biosafety, Select Agent and Toxin Security, Animal Care and Use, the Protection of Human Subjects, Life Sciences Dual Use Research of Concern, and Export Controls.

CAPO collects and reviews relevant documentation pertaining to this Award on behalf of the CAPM. Additional guidance regarding the review process is provided in the following sections, along with contact information for the TCO, RCO, and ECG. This guidance applies to the Recipient and any/all Recipient

institutions involved in the performance of work under this Award.

The Recipient is responsible for ensuring that any/all Recipient institutions and collaborators comply with all requirements and submit relevant documentation for work being performed under this Award.

## C. SECURITY REQUIREMENTS

Recipient access to Controlled Unclassified Information will be required under this Award for approximately 140 Recipient personnel. Approximately 30 Recipient personnel will require access to Top Secret classified information and access to Sensitive Compartmented Information (SCI). These Recipient personnel must obtain and retain a Top Secret clearance and retain SCI eligibility/access during the performance of the Award. Section III.E below sets forth further details concerning the Classified Security Conditions.

Department of Homeland Security Acquisition Regulation (HSAR) clause 3052.204-71 requires that Recipient personnel requiring unescorted access to Government facilities, access to sensitive information, or access to Government information technology (IT) resources are required to have a favorably adjudicated background investigation prior to commencing work. HSAR clause 3052.204-71 also provides the definition of "sensitive information" that is applicable to this agreement. See 48 C.F.R. § 3052.204-71.

DHS/CISA policy requires a favorably adjudicated background investigation prior to commencing work on this cooperative agreement, for all personnel who require recurring access to Government facilities and access to sensitive information, or access to Government IT resources. These role-based personnel must be U.S. citizens and must be subject to a fitness determination made by the DHS/CISA Personnel Security Division. Recipient employees assigned to perform a task under this Award will be given a fitness determination unless this requirement is waived under Departmental procedures.

The DHS/CISA Office of the Chief Security Officer (OCSO) has primary security cognizance of all work performed during the performance of this Award unless otherwise directed by the government.

### 1. EMPLOYMENT ELIGIBILITY

The Recipient must agree that each employee working on this Award with access to Government facilities and access to sensitive information, or access to Government IT resources, will have a Social Security Card issued and approved by the Social Security Administration. The Recipient is responsible to the Government for acts and omissions of its own employees and for any contractor(s) and their employees.

Subject to existing law, regulations and/or other provisions of this Award, persons without legal immigration status must not be employed by the Recipient, or with this Award. The Recipient must ensure that this provision is expressly incorporated into any and all contracts or subordinate agreements issued in support of this Award.

### 2. CONTINUED ELIGIBILITY

- a. The PO may require the Recipient to prohibit individuals from working on this Award if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to carelessness, insubordination, incompetence, and/or security concerns.
- b. If a prospective employee is found to be ineligible for access to Government facilities or information, the PO will advise the Recipient that the employee shall not continue to work or to be assigned to work under the Award.
- c. The Recipient must report any adverse information coming to their attention concerning employees under the Award to DHS/CISA Security Office. Reports based on rumor or innuendo should not be

made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report must include the employee's name and social security number, along with the adverse information being reported.

- d. The DHS/CISA Security Office must be notified of all terminations/resignations within five days of occurrence. The Recipient must return any expired DHS/CISA issued identification cards and building passes, or those of terminated employees to the PO. If an identification card or building pass is not available to be returned, a report must be submitted to the PO referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card.

### 3. FITNESS DETERMINATION

CISA will have and exercise full control over granting, denying, withholding, or terminating unescorted government facility and/or sensitive Government information access for Recipient employees, based upon the results of a background investigation. CISA may, as it deems appropriate, authorize, and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the final fitness determination and/or full investigation. The granting of a favorable EOD decision will not be considered as assurance that a favorable final fitness determination will follow as a result thereof. The granting of a favorable EOD decision or a final fitness determination will in no way prevent, preclude, or bar the withdrawal or termination of any such access by CISA, at any time during the term of the Award. No employee of the Recipient will be allowed unescorted access to a Government facility without a favorable EOD decision or fitness determination by the Security Office. Recipient employees assigned to the Award not needing access to classified information, Controlled Unclassified Information, and Sensitive But Unclassified information or recurring access to CISA's facilities will not be subject to security suitability screening.

Recipient employees awaiting an EOD decision may begin work on the Award provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if the Recipient is escorted by a government employee. This limited access is to allow Recipient employees to attend briefings and non-recurring meetings and begin transition work.

### 4. BACKGROUND INVESTIGATIONS

Recipient employees (to include applicants, temporary, part-time, and replacement employees) under the Award, needing access to sensitive information, will undergo a position sensitivity analysis based on the duties each individual will perform on the task order. PIV cards will be required for all staff assigned to government facilities under this Award. The Program Office will provide the employees with the proper security paperwork for obtaining the PIV cards and will ensure that all PIV cards are returned at the end of the cooperative agreement. The results of the position sensitivity analysis will identify the appropriate background investigation to be conducted.

- a. All background investigations will be processed through the Security Office. Prospective employees shall submit the following completed forms to the Security Office through the COR (Contract Representative) no less than thirty (30) days before the starting date of the Award or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:
  - i. Standard Form 85P, "Questionnaire for Public Trust Positions"
  - ii. FD Form 258, "Fingerprint Card" (2 copies)
  - iii. Conditional Access to Sensitive but Unclassified Information
  - iv. Non-Disclosure Agreement
  - v. Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act
- b. Required forms will be provided by CISA at the time of Award. Only complete packages will be



accepted by the Security Office. Specific instructions on submission of packages will be provided upon Award.

- c. Be advised that unless an applicant requiring access to sensitive information has resided in the US for three (3) of the past five (5) years, the Government may not be able to complete a satisfactory background investigation. In such cases, CISA retains the right to deem an applicant as ineligible due to insufficient background information.
  - d. The use of non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this Award for any position that involves access to or development of any CISA IT system or access to Federal sensitive information. CISA shall not approve LPRs for employment on this Award in any position that requires the LPR to access or assist in the development, operation, Management, or maintenance of CISA IT systems and/or sensitive information. By signing this Award, the Recipient agrees to this restriction. In those instances where other non-IT requirements contained in the Award can be met by using LPRs, those requirements shall be clearly described.
5. The security requirements for this Award order include:
- a. Personnel security
  - b. Information technology security
  - c. Facility security
6. The following security clauses are incorporated by reference:
- a. FAR 52.204-2, Security Requirements (MAR 2021)
  - b. FAR 52.204-9, Personal Identity Verification of Contractor Personnel (MAR 2023)
  - c. HSAR 3052.204-71, Contractor Employee Access (SEP 2012), ALTERNATE I (SEP 2012)
  - d. Safeguarding of Sensitive Information (MAR 2015)
  - e. Information Technology Security and Privacy Training (MAY 2020)

#### **D. COMPLIANCE WITH INFORMATION SYSTEMS SECURITY**

Security for all information technology (IT) systems employed in the performance of this Award, including equipment and information, is the Recipient's responsibility.

For covered information systems that are not part of an information technology service or system operated on behalf of the Government (see DFAR 252.204-7012(b)(2))—

1. The Recipient must ensure that this provision is expressly incorporated into any and all contracts or subordinate agreements issued in support of this Award.
2. The Recipient represents that it will implement the security measures required by the Federal Information Security Modernization Act of 2014, including those measures detailed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 1 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see <http://dx.doi.org/10.6028/NIST.SP.800-171>) (NIST SP 800-171) and are in effect at the time the Award is issued.
3. a. If the Recipient proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the Award is issued, the Recipient must submit to the Program Officer, for consideration by the CISA Chief Information Security Officer (CISO), a written explanation of—
  - i. Why a particular security requirement is not applicable; or

- ii. How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.
  - b. An authorized representative of the CISA CISO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting Award.
4. The Recipient agrees that when collecting and managing data under this cooperative agreement, it will protect the data by following all applicable state law cybersecurity requirements.
5. If the Recipient intends to use an external cloud service provider to store, process, or transmit any covered Government information in performance of this Award, the Recipient must require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (<https://www.fedramp.gov/documents-templates/>) and that the cloud service provider complies with requirements of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment. These measures may be addressed in a system security plan.
6. CISA will ensure that any connections between the Recipient's network or information system and CISA networks used by the Recipient to transfer data under this cooperative agreement are secure. For purposes of this Section, a connection is defined as a dedicated persistent interface between an Agency IT system and an external IT system for the purpose of transferring information. Transitory, user-controlled connections such as website browsing are excluded from this definition. The Recipient agrees to ensure that any connections meet DHS/CISA security requirements, including entering into Interconnection Service Agreements as appropriate. This condition does not apply to manual entry of data by the Recipient into systems operated and used by DHS/CISA's programs for the submission of reporting and/or compliance data.
7. Supply Chain Risk
- a. Government reserves the right to complete a review of the supply chain risk and conduct a risk assessment at any time during this Award. Such risk assessment may include reviewing any contractors, suppliers, distributors, and manufacturers involved in the Awardee's supply chain. Upon written notification from government, within 10 days or a reasonable amount of time as determined by the Grants Officer, the Recipient must provide any information government deems necessary to facilitate its Supply Chain Risk Assessment. If the Recipient believes that the information government requests contain confidential information, the Recipient may state its justification for designating the information as confidential and request that government and any third-party vendor it may use sign a confidentiality agreement before releasing the information. Designation of information as confidential does not give the Recipient the right to withhold the information. As deemed necessary, government may contract with a third party to assist in the review of the supply chain risk assessment.
  - b. Government may request the following information (or other information if deemed necessary) from the apparent Awardee:
    - i. The identity of the apparent Awardee's parent and/or subsidiary corporate entities.
    - ii. The identity of any proposed contractors (including but not limited to suppliers, distributors, and manufacturers) involved in its supply chain.

- iii. The degree of any foreign ownership in or control of the entities identified under (i) and (ii) above.
- iv. The names and dates of birth of the apparent Awardee's corporate officers identified under (i) or (ii), including this information for subcontractors (including but not limited to suppliers, distributors, and manufacturers).
- v. Whether the Award Recipient and contractors (including but not limited to suppliers, distributors, and manufacturers), maintain a formal security program that includes:
  - 1) Personnel security;
  - 2) Physical security program;
  - 3) Information Technology security program; and
  - 4) Supply chain risk management program.
- vi. The name and locations of each facility where any information system, information technology hardware and/or software to be delivered under the Award was designed, manufactured, packaged, and stored prior to distribution.
- vii. The means and method for delivering any information system, information technology hardware (including but not limited to storage subsystems including hardware for software defined subsystems, switches and directors, de-duplication appliances, and storage virtualization appliances), and/or software to be delivered under the Award, including the names of any entity responsible for transport or storage. This information should address whether the information system, information technology hardware and/or software will be direct shipped to Government.
- viii. Whether the proposed information system, information technology hardware and/or software includes a service agreement required by the Award, and if so, the identity of the contractor/subcontractor(s) who will provide this follow-on service, and how the services will be delivered/deployed (e.g., via on-site service? Remotely via internet?).
- ix. The identity of the entity that will provide disposal services of any information system, information technology hardware, and/or software required by the Award.

8. Cyber incident reporting requirement.

a. When the Recipient discovers a cyber incident that affects a covered Recipient information system or the covered Government information residing therein, or that affects the Recipient's ability to perform the requirements of the Award that are designated as operationally critical support, the Recipient must—

- i. Conduct a review for evidence of compromise of covered Government information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered information system(s) that were part of the cyber incident, as well as other information systems on the network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Recipient's ability to provide operationally critical support; and
- ii. Rapidly report cyber incidents to CISA PO at <https://www.cisa.gov/forms/report>.

b. Reporting of a Cyber incident involving classified networks or possible access, or spillage of classified information must be reported to the CISA Industrial Security Program identified in Section E.

9. Within a time mutually agreed upon by the Awardee and the cognizant Program Officer, the Recipient must provide a written Summary of the policies, procedures, and practices employed by the Recipient as



part of the Awardee's IT security program, in place or planned, to protect activities in support of the Award.

The Summary must describe the information security program appropriate for the program including, but not limited to: roles and responsibilities, risk assessment, technical safeguards, administrative safeguards, physical safeguards, policies and procedures, awareness and training and notification procedures in the event of a cyber-security breach. The Summary must include the Recipient's evaluation criteria that will measure the successful implementation of the IT Security Program. In addition, the Summary must address appropriate security measures required of all sub Recipients, researchers, and others who will have access to the systems employed in support of this Award.

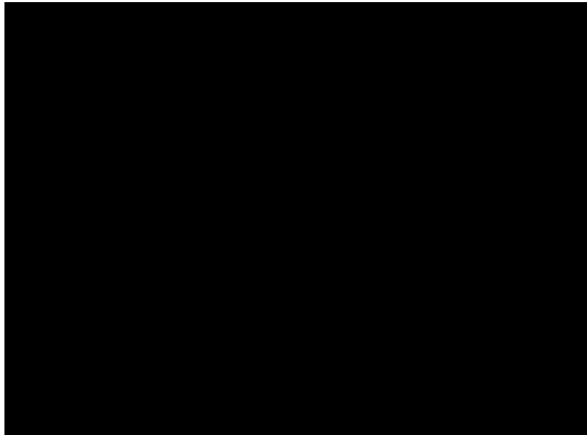
The Summary will be the basis of a dialogue which CISA PO will have with the Recipient, directly or through meetings. Discussions will address a number of topics, such as, but not limited to, evolving security concerns and concomitant cyber-security policy and procedures within the Government and at the Recipient, available education and training activities in cybersecurity, and coordination activities.

## E. CLASSIFIED SECURITY CONDITIONS

1. "Classified national security information," as defined in Executive Order (EO) 12958, as amended, means information that has been determined pursuant to EO 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
2. The details concerning the classified security conditions for the Award will be specified in a Department of Defense (DD) Form 254.
3. Approximately 30 Recipient personnel will require access to Top Secret classified information and access to Sensitive Compartmented Information (SCI) under this Award. These personnel must obtain and retain a Top Secret clearance and obtain and retain SCI eligibility/access during the period of performance of the Award.
4. The Recipient must obtain and maintain an active final Top Secret facility clearance (FCL) granted by the Defense Counterintelligence and Security Agency (DCSA) for the Recipient's location. There does not need to be a Safeguarding Level. DHS will not accept interim FCLs.
5. No SCI activities will occur at the Recipient location until the facility has been accredited by DHS or a co-utilization agreement is made between DHS and the current facility Government accrediting authority. DHS accreditation of an SCI Facility must be requested via the DHS Office of Security of Determination Authority and Cognizant Security Authority at [REDACTED]. The request for accreditation will include a concept of operations (CONOPS) which describes the operational requirement, facility description, and security oversight. Upon approval of the CONOPS, a fixed facility checklist and Standard Operating Procedures will be submitted for review and approval. Co-utilization agreement will be requested by the Recipient to the current accrediting authority and coordinated with DHS/OCSO. A copy of the approved co-utilization agreement will be provided to DHS/OCSO/SSPD prior to SCI activities occurring at the Recipient location.
6. **Place of Performance.** The Recipient's personnel will access Top Secret and SCI information at the Recipient's location identified below. They will access this classified information in a DHS accredited SCIF at this location; there will be no storage outside the SCIF.

East Greenbush, NY 12061

7. **Place of Performance.** The Recipient's personnel will access Top Secret and SCI classified information at the following three federal government locations. They will access this classified information in a SCIF at these three locations. No storage is required for Recipient's personnel at these locations.



8. Office of the Chief Security Officer provides approval, guidance, and oversight for receiving, generating, and storing classified information.

9. No funding under this Award shall be used to support a contract, sub-award, or other agreement for goods or services that will include access to classified national security information if the Award Recipient itself has not been approved for and has access to such information.

10. Where a Recipient has been approved for and has access to classified national security information, no funding under this Award shall be used to support a contract, sub-Award, or other agreement for goods or services that will include access to classified national security information by the contractor, subrecipient- or other entity without prior written approval from the DHS Office of Security, Industrial Security Program Branch (ISPB), or, an appropriate official within the Federal department or agency with whom the classified effort will be performed

11. Such contracts, sub-awards, or other agreements must be processed and administered in accordance with the DHS "Standard Operating Procedures, Classified Contracting by State and Local Entities," dated July 7, 2008; EOs 12829, 12958, 12968, as amended; the *National Industrial Security Program Operating Manual* (NISPOM); and/or other applicable implementing directives, amendments, or instructions.

12. Immediately upon determination by the Recipient that funding under this Award will be used to support such a contract, sub-award, or other agreement, and prior to execution of any actions to facilitate the acquisition of such a contract, sub-award, or other agreement, the Recipient shall contact the CISA Chief Security Officer and OCSO/ISPB, for approval and processing instructions.

DHS Office of Security ISPB contact information: Telephone:

Email:

Mail: Department of Homeland Security Office of the Chief Security Officer  
ATTN: NSSD/Industrial Security Program Branch  
245 Murray Lane, SW Bldg. 410  
Washington, D.C. 20528

13. Sensitive Compartmented Information:

- a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible Special Security Office.
- b. SCI will not be released to Recipient employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated Recipient.
- c. All Recipient personnel requiring access to SCI as part of this Award effort must be approved and indoctrinated by CISA. Requests for Access will be submitted by the government project manager who can validate the justification for access.
- d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).
- e. SCI furnished in support of this cooperative agreement remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the Award, SCI furnished will be returned to the direct custody of the supporting SSO or destroyed in accordance with instructions outlined by the Grants Officer.
- f. Visits by Recipient Personnel will only be certified by CISA when such visits are conducted as part of the cooperative agreement effort.
- g. No SCI activities will occur at the Recipient location until the facility has been accredited by DHS or a co-utilization agreement is made between DHS and the current facility Government accrediting authority. DHS accreditation of an SCI Facility must be requested via the DHS Office of Security of Determination Authority and Cognizant Security Authority at [REDACTED]. The request for accreditation will include a concept of operations (CONOPS) which describes the operational requirement, facility description, and security oversight. Upon approval of the CONOPS, a fixed facility checklist and Standard Operating Procedures will be submitted for review and approval. Co-utilization agreement will be requested by the Recipient to the current accrediting authority and coordinated with DHS/OCSO. A copy of the approved co-utilization agreement will be provided to DHS/OCSO/SSPD prior to SCI activities occurring at the Recipient location.
- h. DHS will inspect all SCI Facilities accredited by DHS, security policies and procedures, and all material generated or processed under the purview of this cooperative agreement:
  - i. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security offices (SSO).
  - ii. SCI will not be released to Recipient employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated Recipient.
  - iii. All Recipient personnel requiring access to SCI as part of this cooperative agreement must be approved and indoctrinated by CISA. Requests for Access will be submitted by the government project manager who can validate the justification for access.
  - iv. Inquiries pertaining to classification guidance on SCI will be directed to the SSO.
  - v. SCI furnished in support of this cooperative agreement remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon

completion or cancellation of the cooperative agreement, SCI furnished will be returned to the direct custody of the supporting SSO or destroyed in accordance with instructions outlined by the Grants Officer.

- vi. Visits by Recipient employees will only be certified by CISA PO when such visits are conducted as part of the cooperative agreement effort.
- vii. SCI will be stored and maintained only in properly accredited facilities at the Recipient location.
- viii. All Recipient requests to process SCI electronically will be sent to the accrediting SSO for coordination through appropriate SCI channels.

## **F. CONTROLLED UNCLASSIFIED INFORMATION**

In addition to classified information, certain types of unclassified information also require application of access and distribution controls and protective measures for a variety of reasons. This information is referred to collectively as Controlled Unclassified Information (CUI). CUI includes but is not limited to: For Official Use Only (FOUO), Law Enforcement Sensitive (LES) and Limited Distribution, as well as some categories developed by other executive branch agencies. Recipient must comply with the Traffic Light Protocol when required by CISA or marked on documents received from/sent to CISA or other entities.

1. All non-Federal entities doing business with CISA are expected to adhere to the following procedural safeguards, in addition to any other relevant federal specific procedures, for any potential business with CISA:
  - a. Do not process CISA CUI on publicly available computers or post CISA CUI to publicly available webpages or websites that have access limited only by domain or Internet protocol restriction.
  - b. Ensure that all CISA CUI is protected by a physical or electronic barrier when not under direct individual control of an authorized user and limit the transfer or CISA CUI to subcontractors or teaming partners with a need to know and commitment to this level of protection.
  - c. Ensure that CISA CUI on mobile computing devices is identified and encrypted, and all communications on mobile devices or through wireless connections are protected and encrypted.
  - d. Overwrite media that has been used to process CISA CUI before external release or disposal.
  - e. The parties understand that information and materials provided pursuant to or resulting from this Award may be export controlled, sensitive, for official use only, or otherwise protected by law, executive order, or regulation. The Recipient is responsible for compliance with all applicable laws and regulations. Nothing in this Award shall be construed to permit any disclosure in violation of those restrictions.

## **G. HANDLING OF INFORMATION**

Recipient will provide CISA PO a detailed briefing on the information handling and protection methodology and protocols to be used by Recipient or its agents, and on the capabilities of the facilities that will be involved in receiving, storing, and processing any unclassified Federal Government analytical products and information provided to Recipient or its agents in consideration of this Agreement.

1. Within the methodology and protocols defined above, Recipient or its agents will ensure that only its personnel,



members, or agents approved by CISA PO who will be directly involved in managing and securing information systems will have access to unclassified, but Sensitive Federal Government information and analytical products.

2. Recipient shall adhere to any dissemination control markings clearly displayed on written documents containing any cybersecurity information shared under this Agreement.
3. Prior to sharing with the Federal Government, Recipient will remove information not directly related to a Cybersecurity Threat the Recipient knows at the time of sharing to be personal information of a specific person.
4. Recipient will ensure that any risk mitigation efforts, including use of Defensive Measures, that are based on government provided information, do not initiate communications with related threat resources defined within government provided information unless the Recipient is acting upon information obtained from other sources or transactions.
5. If Recipient uses government-provided information to enhance cyber threat detection and/or prevention services to third parties not covered by this Award, Recipient must notify CISA of any possible cyber threats detected and/or prevented using this information, as well as the name of each associated third-party entity.
6. With respect to CISA and other federal government provided information that the Recipient disseminates to non-federal entities when carrying out the scope of work under this Award, such information will remain the property of the federal government and is not releasable by the non-federal entities without express CISA authorization. Recipient will communicate that fact to such non-federal entities in order to ensure that, if a state, local, tribal, or territorial (SLTT) government receives a freedom of information or similar request under state, local, or tribal law, that SLTT government is able to appropriately process that request in light of the federal government's ownership of such information and prohibition against releasing that information without express CISA authorization.
7. Unless Recipient and CISA specifically agree otherwise, Recipient will not enter into any new agreement under this Award with a third party that would prohibit Recipient from performing the tasks detailed in Appendix A, including, as applicable, sharing pertinent information with CISA regarding cyber threats, risks, vulnerabilities, and incidents impacting such third party. For purposes of this provision, "new agreement" means an agreement for a service listed in Appendix A funded by this Award and entered into by Recipient and the third party after the beginning of the Project Period of this Award. If Recipient delivers services to any third party under this Award pursuant to a pre-existing agreement that prohibits Recipient from sharing pertinent information with CISA, Recipient will (i) replace or modify the pre-existing agreement such that the pre-existing agreement no longer prohibits Recipient from performing the tasks detailed in Appendix A, including, as applicable, sharing such pertinent information with CISA or (ii) request written permission from CISA for that pre-existing agreement to be excepted from the requirement referenced in (i). For purposes of this provision, "pre-existing agreement" means an agreement for a service listed in Appendix A funded by this Award and entered into by Recipient and the third party before the beginning of the Project Period of this Award.

## **H. NOTICE AND CONSENT CERTIFICATIONS**

1. Recipient must comply with the U.S. Constitution, including the Fourth Amendment, any similar provisions in State Constitutions, and relevant Federal and State-level electronic communications and privacy statutes.
2. Recipient provides security services (including enhanced netflow/IPFIX, intrusion detection and intrusion prevention, endpoint detection and response (EDR)), to state, local, tribal, and territorial governments, and their individual agencies (Recipient Customers). Before providing managed security services including enhanced netflow/IPFIX, intrusion detection, intrusion prevention, endpoint detection and response, or any

other services that potentially acquire the content of electronic communications or data stored on, transiting, or being processed by a network or device, such as Cybersecurity Incident Response Support as described in Appendix A section 4.2.2.1, Recipient will obtain signed certifications substantially similar to the below from each new Recipient Customer. Recipient must obtain multiple certifications from Recipient Customer sub-entities as necessary to ensure that all users for whom such data will potentially be collected are covered by a certification. The certifications must state that Recipient Customer's computer users have received notice and consented to the following:

- a. Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Recipient Customer's information system; and
  - b. All communications and data transitioning, stored on, or traveling to or from the Recipient Customer's information system will be monitored and may be disclosed or used for any lawful government purpose.
3. In the event that certain Recipient Customers request to sign a different form of certification or otherwise request an exception to the requirements in this paragraph, Recipient shall receive CISA approval to modify the requirements of this paragraph. Recipient's point of contact for such requests is OCC\_Cyber@cisa.dhs.gov.
4. Recipient will provide the certifications described above to CISA upon CISA PO request.

## **I. COMPLIANCE WITH U.S. EXPORT CONTROLS**

Activities performed by the Recipient and any Recipient institution under this Award may or may not be subject to U.S. export control regulations. The Recipient and any Recipient institution shall conduct all such activities, to include any and all CISA-funded research and development, acquisitions, and collaborations in full compliance with U.S. export controls-to include the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR), and the Office of Foreign Assets Control (OFAC) Regulations. The Recipient and any Recipient institution will ensure that all legal requirements for compliance with U.S. export controls are met prior to transferring commodities, technologies, technical data, or other controlled information to a non-U.S. person or entity. Upon CISA PO request, the Recipient and any Recipient institution must provide to CAPO documentation and any other information necessary to determine satisfaction of this requirement.

All documentation, as well as any questions or concerns regarding export controls, should be submitted to the RCO at [REDACTED]

## **J. PATENT RIGHTS, DATA RIGHTS, AND TRADEMARKS**

### **1. PATENT RIGHTS**

The Recipient is subject to applicable regulations governing patents and inventions, including government-wide regulations issued by the Department of Commerce at 37 C.F.R. Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements." The standard patents clause at 37 C.F.R. § 401.14 is incorporated by reference. All reports of subject inventions made under this Award should be submitted to CISA using the Interagency Edison system website at <https://www.iedison.gov/>.

### **2. INTELLECTUAL PROPERTY EVALUATION CRITERION (or sub-criterion).**

The operation and maintenance of software p, and any new software acquired under the Award or developed during the Period of Performance of this Award must:

- a. be transparent in design and practice to the Government;



- b. be capable of being seamlessly handed over to a successor Recipient or contractor skilled in the art of computer programming, maintenance, and upgrading, including documentation and licensing of any third-party software components or modules; and,
- c. assure that the ability of the software is contemporaneously archived to assure stability and the ability to survive outages.

The Recipient must present a plan to assure these characteristics and will be evaluated as to the Government's assessment of the completeness and viability of the plan.

### 3. TRADEMARKS

CISA may require the Recipient to provide some or all services under this Award exclusively under the mark and associated logos provided by CISA (collectively, "Marks"). The Recipient is permitted to use the Marks in any manner necessary to achieve the listed program objective including brochures, conference presentations, promotional merchandise, Awards, and digital advertising. For additional uses, the Recipient will confer with the CISA Office of External Affairs, and Office of Chief Counsel. The Recipient will not create, register, or use any additional common law or federal registered marks in reference to the services associated with this Award without prior CISA approval.

### 4. DATA RIGHTS

CISA has the right to:

- a. Obtain, reproduce, publish, or otherwise use the data produced under the Award; and
- b. Authorize others to receive, reproduce, publish, or otherwise use such data for Federal purposes.

## K. COMPUTER SOFTWARE

Any software produced in the course of performance of the Award will conform to the below terms.

### 1. The Recipient will design the computer software under the following bases:

- a. **Commercial or Proprietary Software Components:** Software, especially computer software used for online products and services, must be commercially available off-the-shelf, unless the CISA PO authorizes otherwise. The Recipient may not incorporate into the computer software content that is subject to either commercial or proprietary license conditions without the prior approval of the CISA PO.
- b. **Computer Language:** The Recipient must design and produce the software using the languages and specifications as directed by the CISA PO.
- c. **Open-Source Software Components:** To the extent that the Recipient intends to incorporate open-source content into the computer software, it may use open-source content subject to an open-source license that either requires only acknowledgement of the source or the source and a disclaimer of liability. Prior to incorporating open-source content subject to any other license conditions, the Recipient must request and receive the prior written approval of the CISA PO.

### 2. As part of closeout of the Award and at any times required by CISA during the Period of Performance, the Recipient must provide the following deliverables associated with that computer software:

- a. Operable Source Code: The Recipient must deliver at the conclusion of Award performance one computer disc or make downloadable electronically as directed by the DHS Grants Officer, software containing the complete, easy to compile, and operable source code in the CISA approved language.
  - b. Executable Code: The Recipient must deliver at the conclusion of Award performance one computer disc or make downloadable electronically as directed by the DHS Grants Officer, software containing the complete and operable executable code.
  - c. Software Documentation: The Recipient must create and deliver software documentation that contain programmer notes describing the following:
    - i. The software's operation, organization, and any significant characteristics of its design.
    - ii. The foregoing information provided such that a computer programmer skilled in the art of programming according to the approved language may operate, maintain, update, modify, and perform all operations necessary to perpetuate the utility of the computer software.
  - d. Description of Third-Party Licenses Used: To the extent that the Recipient has included in the computer software, either CISA approved open-source content or software content subject to proprietary licenses, the Recipient must provide each of those licenses and incorporate those licenses in a delivered file.
3. Independence of Cloud Based Software: The Recipient must rely on high-performance computing resources. A key measure of innovation is leveraging the capabilities of cloud computing for analytics, collaboration, and workflow with non-Recipients. The Recipient must ensure that cloud computing software is capable of running on non-Recipient based systems. Any cloud-based software must be capable of running on equivalent CISA or third-party servers. This attribute must be an aspect of the software's underlying design.
4. Interoperability of Related Data: Data derived from the created software must be capable of being transferred to other software in a machine legible format with a minimal level of outside intervention when consistent with standard industry practice. This attribute must be part of the software's underlying design.
5. Testing of Software.
- a. Software Testing Required. Any software created under interagency agreement, contract, other transaction agreement, or cooperative agreement prior to delivery must undergo software testing. Software testing must be conducted using industry standard tools and in the testing environments identified in the Recipient's proposal under the heading titled "Program Management Plan Major Milestone(s)", incorporated herein by reference.
  - b. Timing of Software Testing. Software testing should occur once executable software has been created.
  - c. Software Testing Requirements. Software testing should determine the following:
    - i. That the software can serve the purpose of its creation and meets the requirements.
    - ii. That the software is stable and performs correctly to all inputted information.
    - iii. The software is usable and performs its functions within a time frame appropriate for the nature of the operation.
  - d. Installation Testing. Installation testing that identifies what will be necessary for a user to install and

successfully run the software will be required prior to delivery.

## L. PUBLICATIONS

1. Acknowledgement and Disclaimer. The Recipient agrees to reference CISA investments in the project during all phases of community outreach outlined in the CISA PO approved workplan which may include development of any post-project summary or success materials that highlight achievements to which this project contributed. All publications produced as a result of this Award which are submitted for publication in any magazine, journal, or trade paper must include the following statement:

Acknowledgement. "This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, (XXXXXXXXXXXX)."

Disclaimer. "The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security."

Recipient agrees to include in any subaward made under this Agreement the requirements of this Award term (Publications).

2. Enhancing Public Access to Publications. The Recipient may copyright any work that is subject to copyright and was developed, or for which ownership was acquired, under this Award. CISA reserves a royalty-free, nonexclusive, and irrevocable right to reproduce, publish, or otherwise use the work for federal purposes, and to authorize others to do so pursuant to 2 C.F.R. § 200.315(b). Authors and journals can assert copyright in CISA-funded scientific publications, in accordance with current practice and CISA encourages authors to give CISA a copy of their final manuscript or software before publication. While individual copyright arrangements can take many forms, CISA encourages investigators to sign agreements that specifically allow the manuscript or software to be deposited with CISA for public posting or use after journal publication. Institutions and investigators may wish to develop particular terms in consultation with their own legal counsel, as appropriate. But, as an example, the kind of language that an author or institution might add to a copyright agreement includes the following: "Journal (or Software Recipient) acknowledges that the Author retains the right to provide a final copy of the final manuscript or software application to CISA upon acceptance for Journal publication or thereafter, for public access purposes through CISA's websites or for public archiving purposes."

### 3. Coordination of Public Statements

- a. Any public references to or descriptions of the program activities undertaken under this Agreement by the Recipient, or any Analytical Products produced jointly by the Recipient and CISA PO under this Agreement will be done only after coordination, in writing between the Recipient and CISA PO.
- b. The Recipient must notify the CISA PO of public or media events publicizing the accomplishment of significant events as a result of this agreement and provide the opportunity for attendance and participation by federal representatives with at least ten (10) working days' notice.

## M. SITE VISITS

CISA PO, through authorized representatives, has the right, at all reasonable times, to make site visits to review project accomplishments and management control systems and to provide such technical assistance as may be required. If any site visit is made by CISA PO on the premises of the Recipient, or a



contractor under this Award, the Recipient must provide and must require its contractors to provide all reasonable facilities and assistance for the safety and convenience of the Government representatives in the performance of their duties. All site visits and evaluations will be performed in such a manner that will not unduly delay the work.

## **N. TRAVEL**

Travel required in the performance of the duties approved in this Award must comply with 2 C.F.R. § 200.475. **Foreign travel must be approved by CISA PO in advance and in writing.** Requests for foreign travel identifying the traveler, the purpose, the destination, and the estimated travel costs must be submitted to the DHS Grants Officer 60 days prior to the commencement of travel.

## **O. PUBLIC HEALTH**

Recipient must ensure, to the extent consistent with law, that any Recipient personnel that enter a federal facility in carrying out the scope of work under the Award comply with all applicable public health rules, disclosures, and requirements established for that federal facility.

## **P. TERMINATION**

The Award may be terminated in whole or in part pursuant to 2 C.F.R. § 200.340. All notices are to be transmitted to the DHS Grants Officer via registered or certified mail, return receipt requested. The Recipient's authority to incur new costs will be terminated upon arrival of the date of receipt of the letter or the date set forth in the notice. Any costs incurred up to the earlier of the date of the receipt of the notice or the date of termination set forth in the notice will be negotiated for final payment. When the Award is terminated or partially terminated, the Recipient remains responsible for compliance with the requirements of 2 C.F.R. §§ 200.344 and 345.

Non-Renewal of the Cooperative Agreement:

In the event that CISA PO does not approve a subsequent budget period under this Award and/or does not Award a subsequent cooperative agreement to the Recipient, the Recipient Award agrees to provide for an orderly and efficient transition to any successor recipient.

## **Q. GOVERNING PROVISIONS**

The following are incorporated into this Award by reference:

2 C.F.R. Part 200, Uniform Administrative Requirement, Cost Principles, and Audit Requirements for Federal Awards

NOFO, DHS-23-CISA-123-ISAC000001

Grant Application and Assurances dated September 2023













































































































































































