U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

September 27, 2021

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

Re: Award Number: 19PDMSI00002-03-00
State, Local, Tribal and Territorial (SLTT) Security Operations Center (SOC) | Information Sharing and Analysis Center (ISAC)

Dear [redacted]

The Department of Homeland Security (DHS) has approved your continuation application entitled, "State, Local, Tribal and Territorial (SLTT) Security Operations Center (SOC) | Information Sharing and Analysis Center (ISAC)". Your application was approved in the amount of **$38,211,657** for the period of 9/30/2021 to 9/29/2022. This amount includes a total of $26,344,000 in FY21 Continuation Funding, a total of $11,290,286 in Recipient Cost Share, and a total of $577,371 in estimated FY20 Carryover Funding.

Of the total awarded, **$3,722,089** is restricted from use pending DHS approval, as outlined in the enclosed Terms and Conditions. Additionally, some of the Terms and Conditions have been modified, so please review them carefully in order to effectively execute your award.

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.

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

cc: (via email):

[redacted]

1. DATE ISSUED *MM/DD/YYYY*	**1a. SUPERSEDES AWARD NOTICE dated**
09/27/2021	except that any additions or restrictions previously imposed remain in effect unless specifically rescinded
2. CFDA NO.	
97.123 - Cooperative Agreements	
3. ASSISTANCE TYPE Cooperative Agreement	
4. GRANT NO. 19PDMSI00002-03-00 **Formerly**	**5. TYPE OF AWARD** Other
4a. FAIN 19PDMSI00002	**5a. ACTION TYPE** Non-Competing Continuation
6. PROJECT PERIOD *MM/DD/YYYY* **From** 09/30/2019	**Through** *MM/DD/YYYY* 09/29/2023
7. BUDGET PERIOD *MM/DD/YYYY* **From** 09/30/2021	**Through** *MM/DD/YYYY* 09/29/2022

Department of Homeland Security

DHS Grants and Financial Assistance Division (GFAD)

301 7th Street, SW, RM 3051
Mail Stop 0115
Washington, DC 20528

NOTICE OF AWARD

AUTHORIZATION (Legislation/Regulations)
Homeland Security Act of 2002, Title II, 6 U.S.C. 121(d)

8. TITLE OF PROJECT (OR PROGRAM)
State, Local, Tribal and Territorial (SLTT) Security Operations Center (SOC) | Information Sharing and Analysis Center (ISAC)

9a. GRANTEE NAME AND ADDRESS
Center For Internet Security, Inc.
31 Tech Valley Dr
East Greenbush, NY 12061-4134

9b. GRANTEE PROJECT DIRECTOR
[redacted]
31 Tech Valley Dr
East Greenbush, NY 12061-4134
Phone: 518-516-3018

10a. GRANTEE AUTHORIZING OFFICIAL
[redacted]
31 Tech Valley Dr
East Greenbush, NY 12061-4134
[redacted]

10b. FEDERAL PROJECT OFFICER
[redacted]
7th And D Street SW
Washington, DC 20407-0001
[redacted]

ALL AMOUNTS ARE SHOWN IN USD

11. APPROVED BUDGET (Excludes Direct Assistance)

I Financial Assistance from the Federal Awarding Agency Only		—
II Total project costs including grant funds and all other financial participation		II
a. Salaries and Wages		8,473,855.00
b. Fringe Benefits		1,899,837.00
c. Total Personnel Costs		10,373,692.00
d. Equipment		59,500.00
e. Supplies		19,988.00
f. Travel		360,664.00
g. Construction		0.00
h. Other		15,024,140.00
i. Contractual		0.00
j. TOTAL DIRECT COSTS	25,837,984.00	
k. INDIRECT COSTS	12,373,673.00	
l. **TOTAL APPROVED BUDGET**	38,211,657.00	
m. Federal Share		26,921,371.00
n. Non-Federal Share		11,290,286.00

12. AWARD COMPUTATION

a. Amount of Federal Financial Assistance (from item 11m)	26,921,371.00
b. Less Unobligated Balance From Prior Budget Periods	577,371.00
c. Less Cumulative Prior Award(s) This Budget Period	0.00
d. **AMOUNT OF FINANCIAL ASSISTANCE THIS ACTION**	26,344,000.00
13. Total Federal Funds Awarded to Date for Project Period	60,106,300.00

14. RECOMMENDED FUTURE SUPPORT
(Subject to the availability of funds and satisfactory progress of the project):

YEAR	TOTAL DIRECT COSTS	YEAR	TOTAL DIRECT COSTS
a. 4		d. 7	
b. 5		e. 8	
c. 6		f. 9	

15. PROGRAM INCOME SHALL BE USED IN ACCORD WITH ONE OF THE FOLLOWING ALTERNATIVES:
a. DEDUCTION
b. ADDITIONAL COSTS
c. MATCHING
d. OTHER RESEARCH (Add / Deduct Option)
e. OTHER *(See REMARKS)*

b

16. THIS AWARD IS BASED ON AN APPLICATION SUBMITTED TO, AND AS APPROVED BY, THE FEDERAL AWARDING AGENCY ON THE ABOVE TITLED PROJECT AND IS SUBJECT TO THE TERMS AND CONDITIONS INCORPORATED EITHER DIRECTLY OR BY REFERENCE IN THE FOLLOWING:
a. The grant program legislation
b. The grant program regulations.
c. This award notice including terms and conditions, if any, noted below under REMARKS.
d. Federal administrative requirements, cost principles and audit requirements applicable to this grant.

In the event there are conflicting or otherwise inconsistent policies applicable to the grant, the above order of precedence shall prevail. Acceptance of the grant terms and conditions is acknowledged by the grantee when funds are drawn or otherwise obtained from the grant payment system.

REMARKS (Other Terms and Conditions Attached - ● Yes ○ No)

The Department of Homeland Security (DHS) has approved your continuation application entitled, "State, Local, Tribal and Territorial (SLTT) Security Operations Center (SOC) | Information Sharing and Analysis Center (ISAC)". Your application was approved in the amount of $38,211,657 for the period of 9/30/2021 to 9/29/2022.

GRANTS MANAGEMENT OFFICIAL:
[redacted]
7th and D Street, SW
Washington DC , DC 20407
[redacted]

17.OBJ CLASS 4102	18a. VENDOR CODE 522278213	18b. EIN 522278213	19. DUNS 197891240	20. CONG. DIST. 20
FY-ACCOUNT NO.	**DOCUMENT NO.**	**ADMINISTRATIVE CODE**	**AMT ACTION FIN ASST**	**APPROPRIATION**
21. a. CC147010566	b. PDMSI00002A	c. MSI2	d. $26,344,000.00	e. 7010566
22. a.	b.	c.	d.	e.
23. a.	b.	c.	d.	e.

Federal Financial Report Cycle			
Reporting Period Start Date	Reporting Period End Date	Reporting Type	Reporting Period Due Date
09/30/2019	09/30/2019	Semi-Annual	10/30/2019
10/01/2019	03/31/2020	Semi-Annual	04/30/2020
04/01/2020	09/30/2020	Semi-Annual	10/30/2020
10/01/2020	03/31/2021	Semi-Annual	04/30/2021
04/01/2021	09/30/2021	Semi-Annual	10/30/2021
10/01/2021	03/31/2022	Semi-Annual	04/30/2022
04/01/2022	09/30/2022	Semi-Annual	10/30/2022
10/01/2022	03/31/2023	Semi-Annual	04/30/2023
04/01/2023	09/29/2023	Final	01/27/2024

Performance Progress Report Cycle			
Reporting Period Start Date	Reporting Period End Date	Reporting Type	Reporting Period Due Date
09/30/2019	09/30/2019	Quarterly	10/30/2019
10/01/2019	12/31/2019	Quarterly	01/30/2020
01/01/2020	03/31/2020	Quarterly	04/30/2020
04/01/2020	06/30/2020	Quarterly	07/30/2020
07/01/2020	09/30/2020	Quarterly	10/30/2020
10/01/2020	12/31/2020	Quarterly	01/30/2021
01/01/2021	03/31/2021	Quarterly	04/30/2021
04/01/2021	06/30/2021	Quarterly	07/30/2021
07/01/2021	09/30/2021	Quarterly	10/30/2021
10/01/2021	12/31/2021	Quarterly	01/30/2022
01/01/2022	03/31/2022	Quarterly	04/30/2022
04/01/2022	06/30/2022	Quarterly	07/30/2022
07/01/2022	09/30/2022	Quarterly	10/30/2022
10/01/2022	12/31/2022	Quarterly	01/30/2023
01/01/2023	03/31/2023	Quarterly	04/30/2023
04/01/2023	06/30/2023	Quarterly	07/30/2023
07/01/2023	09/29/2023	Final	01/27/2024

COOPERATIVE AGREEMENT TERMS AND CONDITIONS
GRANTS AND FINANCIAL ASSISTANCE DIVISION (GFAD)

This cooperative agreement funds and sets out the terms and conditions governing a collaborative effort between the DHS and the Center for Internet Security in the execution of Award Number: 19PDMSI00002.

In addition to the DHS Standard Terms and Conditions as outlined here: https://www.dhs.gov/sites/default/files/publications/fy_2021_dhs_standard_terms_and_conditions_version_11.4_dated_02-17-2021.pdf, the following Terms and Conditions apply specifically to this award as administered by the Grants and Financial Assistance Division (GFAD):

ARTICLE I. GENERAL ADMINISTRATIVE TERMS AND CONDITIONS

A. AWARD SPECIFIC TERMS AND CONDITIONS MODIFICATION

1. Incorporation via Reference

The Additional Details, Objectives, and Performance Metrics outlined in Notice of Funding Opportunity DHS-20-CISA-123-ISAC000001 and Appendices, are hereby incorporated via reference, into the Terms and Conditions of this award.

2. Award Restrictions

Of the total funds awarded, $3,722,089 is restricted from use. The recipient shall use the Program Management or the Project and Portfolio Management categories to incur expenses for planning activities related to the following restricted and reserve funds. The reserve and restricted funds shall only be used once the program has been approved by CISA. The restricted funds may only be used as follows:

a. E-mail Security Pilot funds in the amount of $591,000 are restricted until PO approval has been authorized. To request release of funds, the recipient must provide the following data prior to implementing the sourcing strategy:
   i. Assessment of the Supplier Market
   ii. Sourcing/Outsourcing Strategy (to include cost-benefit analysis)
   iii. Technology RoadMap to include a High-Level Operational Concept and Architecture Graphic
   iv. Milestones for Strategy Implementation

b. Annual Multi-State Information Sharing & Analysis Center (MS-ISAC) Membership Meeting and Conference funds in the amount of $500,000 are restricted until PO approval has been authorized. To request release of funds, the recipient must provide the following data prior to committing resources:
   i. Finalized conference planning package
   ii. Choice and cost of venue and services

c. Funds in the amount of $2,631,089 are restricted as Reserve Funds until PO approval has been authorized. To request release of funds, the recipient must provide the following data prior to committing resources:
   i. Provide a justification/business need for how you will be using the Reserve Funds.
   ii. Provide a tentative timeline of the execution dates and rationale of those dates.
   iii. Provide the proposed amount and the breakdown of how the funds will be used.

iv. Outcome of expenditure (benefits/opportunity costs, risks, dependencies, priorities that will be deferred or stopped)

3. Project Milestones, Deliverables, and Timelines
   a. Changes to the Details, Objectives, Performance Metrics and timelines outlined in Appendix A are subject to DHS review and prior approval. Any changes initiated or proposed by the recipient should be submitted for review and approval along with a programmatic justification and budget impact statement.

   b. The CIS submitted PMP establishes technical milestones and deliverables. If the Recipient fails to achieve two or more technical milestones and deliverables, DHS may renegotiate the Statement of Objectives to this Award. In the alternative, DHS 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 suspend or terminate the Award.

4. Monthly Financial Activity-Based Costing (ABC) Report MODIFICATION
   a. The Recipient shall create an activity-based costing model that identifies program activities and assigns the cost of each activity with resources to all program services and according to the actual consumption by each. 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. Monthly ABC Reports shall be submitted no later than the third Monday of the month. Reports shall be emailed to the DHS Program Officer (PO) at [redacted] and uploaded to the GrantSolutions system using the Grant Note feature and guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

5. In-Progress Review (IPR) and Program Management Review (PMR) MODIFICATION
   a. In addition to what is stated in Appendix A and Appendix B, slides for the IPR and PMR must contain accurate and up-to-date information (including but not limited to financial information, operational data and initiative/program status) when sent to CISA. Additionally, a knowledgeable representative from CIS should be on the IPR and PMR calls to answer questions regarding the slides.

B. DHS PROGRAMMATIC INVOLVEMENT

1. DHS may be substantially involved in overseeing and monitoring this cooperative agreement.
   a. Specifically, substantial federal involvement includes administrative activities such as monitoring, reviewing project phases and approving substantive terms in professional services contracts. DHS will not direct or recommend that the recipient enter into a contract with a particular entity.

   b. Substantial DHS involvement may include reviewing financial and program performance reports, monitoring all reporting, record-keeping, and other program requirements.

   c. DHS involvement will also include executing prior approval authority, to ensure adequate stewardship of the federal funds awarded.

   d. DHS will provide administrative assistance related to security clearances necessary to fulfill the scope of work approved by DHS for an award under this funding opportunity announcement.

2. Effects of DHS substantial involvement include:
   a. The recipient and its subrecipients remain responsible for ensuring costs are allowable under 2 CFR Part 200, Subpart E.

3. DHS will provide substantial involvement in the form of technical collaboration or participation in carrying out the scope of work, joint development of outputs, and oversight.

a. DHS 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.

b. DHS 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.

c. DHS representatives will attend and participate in appropriate meetings initiated by the Recipient.

d. DHS 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.

e. DHS will exchange bi-directional cyber threat indicators and information with the ISAC in furtherance of the objectives and priorities delineated in Appendix A in order to enable a collective defense model.

f. For purposes of maintaining cyber situational awareness of issues that affect reliability and resilience of the SLTT, DHS may exchange unattributed and attributed cyber threat landscape information with the ISAC.

g. DHS will make available office space at CISA 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.

h. DHS provides a compartment on the HSIN platform for sharing information with the SLTT community and DHS staff populate the site with shared federal cyber awareness products.

i. DHS will hold equity calls with federal officials and the ISAC on SLTT/Elections victim notification.

j. DHS 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, table top exercises, and technical assistance upon request.

4. Pass-Through Requirements

a. The Recipient shall comply with the timelines and substantive requirements applicable to federal agencies in the Federal Incident Notification Guidelines (FING) and successor documents or other requirements for any incidents involving Recipient or contractor systems used in performance of the cooperative agreement. The Recipient shall, to the greatest extent practicable, insert a clause containing all the provisions of this clause, including this paragraph, in all contracts for systems used in performance of the cooperative agreement.

b. The Recipient shall, in the event of a known or suspected cybersecurity incident impacting its corporate network, execute a request for technical assistance (RTA) from DHS CISA, thereby permitting CISA to investigate the incident impacting Recipient's corporate network, including through CISA's

deployment of a cyber threat hunting capability to search for indicators of compromise in any Recipient or contractor systems used in performance of the cooperative agreement and to detect, track, and disrupt threats that evade existing controls on Recipient's corporate network. Subject to the terms of the aforementioned RTA, such investigation and/or threat hunting activities include, but are not necessarily limited to, access to administrative networks, systems, and accounts; access to underlying infrastructure systems; and all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. Threat hunting activities may also include: inspections, investigations, forensic reviews, and data analyses and processing. DHS CISA, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response and threat hunting activities. The Recipient shall, to the greatest extent practicable, insert a clause containing all the provisions of this clause, including this paragraph, in all contracts for systems used in performance of the cooperative agreement.

c. In the event that one of Recipient's members requests technical assistance from CISA for hunt or incident response services, and such member requests that Recipient share any of that member's data with CISA, Recipient shall share that member's data consistent with the member's request.

d. The Recipient shall share cyber threat indicators (as defined at 6 U.S.C. § 1501(6)) with any and all available associated context and defensive measures (as defined at 6 U.S.C. § 1501(7)) in an automated fashion using CISA's Automated Indicator Sharing (AIS) platform or successor technology for mitigated and non-mitigated events with a cyber nexus.

e. The Recipient shall comply with Binding Operational Directives (BOD) and Emergency Directives (ED) that CISA identifies in writing to Recipient as relevant to Recipient's security posture. At CISA's request, Recipient shall provide a report on compliance with such BODs and EDs. Below are the first set of BODs and EDs that CISA has identified as relevant to Recipient's security posture.

- ED 21-04 - Mitigate Windows Print Spooler Service Vulnerability
- ED 21-03 - Mitigate Pulse Connect Secure Product Vulnerabilities
- ED 21-02 - Mitigate Microsoft Exchange On-Premises Product Vulnerabilities (unless March 2021 security updates have been applied to all Microsoft Exchange servers)
- ED 21-01 - Mitigate SolarWinds Orion Code Compromise
- ED 20-04 - Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday
- ED 20-03 - Mitigate Windows DNS Server Vulnerability from July 2020 Patch Tuesday
- ED 20-02 - Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday
- ED 19-01 - Mitigate DNS Infrastructure Tampering
- BOD 19-02 - Vulnerability Remediation Requirements for Internet-Accessible Systems
- BOD 18-01 - Enhance Email and Web Security
- BOD 17-01 - Removal of Kaspersky-branded Products
- BOD 16-02 - Threat to Network Infrastructure Devices

CISA will periodically review all BODs and EDs to identify those that are relevant (or no longer relevant) to Recipient's security posture. The Recipient shall provide CISA with the report by the date requested by CISA and include a statement regarding the Recipient's approach to implementing the BOD or ED (e.g., the BOD or ED has been implemented, or a compensating control or other mitigation is in place.)

C. 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 DHS Grants Officer.

b. The Recipient shall obtain prior written approval from the DHS Grants Officer for any budget revision that would result in the need for additional resources/funds.

c. To avoid expenditures on products and services duplicating DHS capabilities or products/services that are already commercially available, the Recipient must obtain the written approval from DHS Project Officer prior to the development of new services delivered to SLTT stakeholders that are not outlined in the approved budget or are otherwise available. DHS 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. Extensions to the Period of Performance can only be authorized in writing by the DHS Grants Officer.

b. The extension request shall be submitted to the DHS Grants Officer sixty (60) days prior to the expiration date of the performance period.

c. Requests for time extensions to the Period of Performance will be considered, but will not be granted 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, extension requests shall not be processed.

d. DHS has no obligation to provide additional resources/funding as a result of an extension.

D. FINANCIAL REPORTS MODIFICATION

1. Financial Reporting Accounting – the Recipient shall provide a clear composition of their spending within the MS-ISAC CORE, Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) CORE, shared services/required functionalities, pilots, new programs, and individual initiatives. The clear breakdown of these funds should be applied to the following, but not be limited to: In-Progress Reviews (IPRs), Program Management Reviews (PMRs), ABC reports, Quarterly Federal Financial Reports, Semi-Annual Federal Financial Reports, Final Federal Financial Reports. The recipient shall work with the Program Officer to define an agreed-upon template for reporting fiscal year's financial breakdowns that will include at minimum cumulative expenditures, monthly expenditures, and monthly forecasts.

2. Semi-Annual Federal Financial Reports – the Recipient shall submit a Federal Financial Report (SF425) to the DHS 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 shall be submitted electronically via www.GrantSolutions.gov. Please select the FFR submission guidance found here: https://www.Grantsolutions.gov/support/granteeUsers.html

3. Final Federal Financial Report –the Recipient shall submit the final Federal Financial Report (SF425) to the DHS Grants Officer no later than 90 days after the end of the Project Period end date. The report shall be submitted electronically via www.GrantSolutions.gov. Please select the FFR submission guidance found

here: https://www.Grantsolutions.gov/support/granteeUsers.html

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

E. PERIOD OF PERFORMANCE

The approved Project and Budget Periods for the supported activity is contingent on the following:

1. Acceptable performance of the program as determined by the Department of Homeland Security (DHS);

2. If applicable, acceptance and approval of each non-competing continuation application by the DHS;

3. Subject to the availability of annual DHS appropriated funds.

F. PERFORMANCE REPORTS MODIFICATION

1. Quarterly and Annual Performance Reports – the Recipient shall submit performance reports to the DHS 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 shall 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 shall 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-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-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 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-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. For submission of this information, complete the Performance Progress Report (PPR) found at: Standard Form - Performance Progress Report (SF-PPR) - OMB 0970-0334.

5. In accordance with 2 CFR 200.328(d)(1), the Recipient agrees to inform DHS as soon as problems, delays, or adverse conditions become known which will impair the ability to meet the outcomes specified in the DHS-approved workplan.

6. Final Performance Report - the Recipient shall submit the Final Performance Report to the DHS Grants Officer no later than 90 days after the expiration of the Project Period. The report shall be submitted via GrantSolutions using the Help/Support Reference entitled, Grant Recipient Process: Performance Progress Reporting.

G. EQUIPMENT

1. Title to equipment acquired by the Recipient with Federal funds provided under this Award shall vest in the Recipient, subject to the conditions pertaining to equipment in the 2 C.F.R. Part 200.

2. Prior to the purchase of Equipment in the amount of $5,000 or more per unit cost, the recipient must obtain the written approval from the DHS Program Officer.

3. For equipment purchased with Award funds having a $5,000 or more per unit cost, the Recipient shall submit an inventory that will include 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. This report will be maintained and due with the Quarterly Performance Reports, and shall be submitted electronically via www.GrantSolutions.gov using the Grant Note feature and guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

4. When equipment acquired under a Federal award is no longer needed, the Recipient entity must obtain disposition instructions from DHS.

H. PAYMENT

1. The Recipient shall 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 the DHS 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.

I. PRIOR APPROVAL REQUIRED

The Recipient shall not, without the prior written approval of the DHS, request reimbursement, incur costs or obligate funds for any purpose pertaining to the operation of the project, program, or activities prior to the approved Budget Period. The recipient shall also adhere to all other prior approval requirements outlined in Article I.

ARTICLE II. GENERAL TERMS AND CONDITIONS

A. ACCESS TO RECORDS.

The Recipient shall retain financial records, supporting documents, statistical records, and all other records pertinent to this Award for a period of three years from the date of submission of the final expenditure report. The only exceptions to the aforementioned record retention requirements are the following:

1. If any litigation, dispute, or audit is started before the expiration of the 3-year period, the records shall be retained until all litigation, dispute or audit findings involving the records have been resolved and final action taken.

2. Records for real property and equipment acquired with Federal funds shall be retained for three (3) years after final disposition.

3. The DHS Grants Officer may direct the Recipient to transfer certain records to DHS custody when he or she determines that the records possess long term retention value. However, in order to avoid duplicate recordkeeping, the DHS Grants Officer may make arrangements for the Recipient to retain any records that are continuously needed for joint use.

4. DHS, the Inspector General, Comptroller General of the United States, or any of their duly authorized representatives, have the right of timely and unrestricted access to any books, documents, papers, or other records of the Recipient that are pertinent to this Award, in order to make audits, examinations, excerpts, transcripts and copies of such documents. This right also includes timely and reasonable access to Recipient's 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 shall last as long as records are retained.

5. With respect to sub-recipients, DHS shall retain the right to conduct a financial review, require an audit, or otherwise ensure adequate accountability of organizations expending DHS funds. Recipient agrees to include in any sub-award made under this Agreement 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 Compliance Assurance Program Manager. 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 classified information and unclassified, but Sensitive Information may be required under this award. The maximum level of classification is Top Secret/SCI. The details will be specified in a Department of Defense (DD) Form 254.

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.

DHS 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 shall be U.S. citizens and shall be subject to a fitness determination made by the DHS Personnel Security Division. Recipient employees will be given a fitness determination unless this requirement is waived under Departmental procedures.

The DHS 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, shall have a Social Security Card issued and approved by the Social Security Administration. The Recipient shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees.

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

2. CONTINUED ELIGIBILITY

   a. The Program Officer (PO) may require the recipient to prohibit individuals from working on this task order 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 shall advise the Recipient that the employee shall not continue to work or to be assigned to work under the award.

   c. The Recipient shall report any adverse information coming to their attention concerning employees under the award to DHS' 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 shall include the employee's name and social security number, along with the adverse information being reported.

   d. The Security Office must be notified of all terminations/resignations within five days of occurrence. The Recipient shall return any expired DHS 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

DHS shall 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. DHS 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 shall not be considered as assurance that a favorable final fitness determination shall follow as a result thereof. The granting of a favorable EOD decision or a final fitness determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the task order. No employee of the Recipient shall 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 sensitive DHS information or recurring access to DHS' facilities shall 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, 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, shall undergo a position sensitivity analysis based on the duties each individual shall perform on the task order. All of the Recipients' employees will be required to undergo DHS fitness investigation. 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 contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted.

a. All background investigations shall 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 shall be provided by DHS at the time of award. Only complete packages shall be accepted by the Security Office. Specific instructions on submission of packages shall 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, DHS 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 DHS IT system or access to Federal sensitive information. DHS 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 DHS 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

Standard U.S. Government security clauses will apply. The following Security clauses are included:
   a. FAR 52.204-2, Security Requirements (AUG 1996)
   b. FAR 52.204-9, Personal Identity Verification of Contractor Personnel (JAN 2011)
   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 (MAR 2015)

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 252.204-7012(b)(2)—

1. 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.

2. 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 shall submit to the Program Officer, for consideration by the DHS 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 DHS 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.

3. 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.

4. 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 shall 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/resources/documents/) 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.

5. DHS must ensure that any connections between the recipient's network or information system and DHS networks used by the recipient to transfer data under this 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 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's programs for the submission of reporting and/or compliance data.

6. 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 subcontractors, 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 shall provide any information government deems necessary to facilitate its Supply Chain Risk Assessment. If the Recipient believes that the information government requests contains 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.

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 subcontractors (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 (1) and (2) above.

iv. The names and dates of birth of the apparent awardee's corporate officers identified under (1) or (2), including this information for subcontractors (including but not limited to suppliers, distributors, and manufacturers).

v. Whether the apparent awardee and subcontractors (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.

7. 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 shall—

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 DHS CISA at https://www.us-cert.gov/forms/report and the DHS CISA Program Officer.

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

8. Within a time mutually agreed upon by the awardee and the cognizant Program Officer, the recipient shall 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 shall 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 shall include the recipient's evaluation criteria that will measure the successful implementation of the IT Security Program. In addition, the Summary shall 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 DHS 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 CONDITION

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. Recipient access to classified information is required under this Cooperative Agreement. Before access to classified information is allowed, a Facility Clearance will be attained and individuals accessing classified will have eligibility determined through the personnel security process. The maximum level of classification

is Top Secret/SCI. The details will be specified in a Department of Defense (DD) Form 254. Accordingly, specified DHS CISA liaison/analyst employees provided for this requirement must be eligible for a Top Secret/SCI Clearance.

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

4. 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 awardrecipient itself has not been approved for and has access to such information.

5. Where an award 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, sub-awardee 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.

6. Such contracts, sub-awards, or other agreements shall 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 or instructions.

7. Immediately upon determination by the award 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 award recipient shall contact the CISA Chief Security Officer and OCSO/ISPB, for approval and processing instructions.

DHS Office of Security ISPB contact information:

Telephone: 202-447-5346

Email: [redacted]

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

8. 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 (SSO).

   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 DHS. Requests for Access will be submitted by the government project manager who can validate the justification foraccess.

   d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).

   e. SCI furnished in support of this contract 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 IAW instructions outlined by the Contract Officer.

f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract 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 the Chief Security Officer, Physical Security Division, Security Projects Branch 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 contractor 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 contractor 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 contract:

   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 contractor 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 contractor.

   iii. All Recipient personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. 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 contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.

   vi. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract 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.

1. All non-Federal entities doing business with DHS CISA are expected to adhere to the following procedural safeguards, in addition to any other relevant federal specific procedures, for any potential business with DHS CISA:

a. Do not process DHS CISA CUI on publicly available computers or post DHS CISA CUI to publicly available webpages or websites that have access limited only by domain or Internet protocol restriction.

b. Ensure that all DHS 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 DHS CISA CUI to subcontractors or teaming partners with a need to know and commitment to this level of protection.

c. Ensure that DHS 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 DHS 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 inviolation of those restrictions.

G. HANDLING OF INFORMATION

Recipient will provide DHS 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 facilitates 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 DHS CISA 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.

H. NOTICE AND CONSENT CERTIFICATIONS

1. Recipient shall comply with the U.S. Constitution, including the Fourth Amendment thereof, 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 shall 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 shall 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 transiting or 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 DHS approval to modify the requirements of this paragraph. Recipient's point of contact for such requests is ogc-cyber@hq.dhs.gov.

4. Recipient will provide the certifications described above to DHS upon DHS's 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 DHS-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 DHS 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 AND DATA RIGHTS

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 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements." The clause at 37 CFR 401.14 is incorporated by reference herein. All reports of subject inventions made under this Award should be submitted to DHS using the Interagency Edison system website at https://public.era.nih.gov/iedison .

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

The services sought under this solicitation are critical to the mission of the Department of Homeland Security's (DHS's) Cybersecurity and Infrastructure Security Agency (CISA) and other Federal agencies. The operation and maintenance of existing software previously funded by DHS and any new software acquired with DHS funds 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 awardee 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 offeror's proposal 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. DATA RIGHTS.

a. The Recipient grants the Government a royalty free, nonexclusive and irrevocable license to reproduce, display, distribute copies, perform, disseminate, or prepare derivative works, and to authorize others to do so, for Government purposes in:

i. Any data that is first produced under this Award and to the Government;

ii. Any data requested in paragraph 3b below, if incorporated in the Award.

"Data" means recorded information, regardless of form or the media on which it may be recorded.

b. Additional requirement for this Award:

i. If the Government believes that it needs additional research data that was produced under this Award, the Government may request the research data and the Recipient agrees to provide the research data within a reasonable time.

ii. The requirement in paragraph 3b.i of this section applies to any research data that are:

1) Produced under this Award, either as a Recipient or sub-recipient;
2) Used by the Government in developing an agency action that has the force and effect of law; and
3) Published, which occurs either when:
   - The research data is published in a peer-reviewed scientific or technical journal; or
   - DHS publicly and officially cites the research data in support of an agency action that has the force and effect of law

c. For the purposes of this section, "research data":

i. Means the recorded factual material {excluding physical objects, such as laboratory samples) commonly accepted in the scientific community as necessary to validate research findings.

ii. Excludes:
   - Preliminary analyses;

- Drafts of scientific papers;
- Plans for future research;
- Peer reviews;
- Communications with colleagues;
- Trade secrets;
- Commercial information;
- Materials necessary that a researcher must hold confidential until
- they are published, or similar information which is protected under law; and
- Personnel and medical information and similar information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, such as information that could be used to identify a particular person in a research study.

d. Requirements for sub-awards:

i. The Recipient agrees to include in any sub-award made under this Agreement the requirements of this award term (Patent Rights and Data Rights) and the **DHS Standard Terms and Conditions** award term (Copyright).

ii. The Recipient should use competition, to the maximum extent possible, when awarding Sub-awards. In addition, the Recipient must give the Federal Awarding Agency its procurement documentation, upon request, when making a non-competitive award over the "simplified acquisition threshold" See 2 C.F.R 200.324.

iii. Sub-awards awarded after the Cooperative Agreement is signed, and not proposed in the application, must be awarded using a formal competitive bidding process. Sub-awards are subject to audit, in accordance with the requirements of 2 C.F.R. Part 200.

e. The Recipient acknowledges that that it may only submit data which it has the legal authority to share. The Recipient shall hold harmless, defend, and indemnify the DHS against any and all third-party data accidently submitted that is subject to copyright, and third-party claims or liabilities addressed within the scope of this Award.

K. COMPUTER SOFTWARE

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

1. The Government will receive unlimited use rights in all computer software resulting directly and solely from the performance of work supported by this Agreement, or any other subcontract or agreement. Unlimited rights, as used in this clause, means rights to use, duplicate, release, or disclose technical data or computer software, in whole or in part, in any manner and for any purpose whatsoever, and to have or permit others to do so.

2. 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 DHS Project Officer authorize otherwise. The Recipient shall not incorporate into the computer software content that is subject to either commercial or proprietary license conditions without the prior approval of the DHS Project Officer.

b. Computer Language: The Recipient shall design and produce the software using the languages and specifications as directed by the DHS Project Officer.

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 DHS Project Officer.

3. Upon conclusion of award performance and at any times specified by the contract during contract performance, the Recipient shall provide the following deliverables associated with that computer software:

a. Operable Source Code: The Recipient shall 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, compilable, and operable source code in the DHS approved language.

b. Executable Code: The Recipient will 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 shall 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 DHS approved open source content or software content subject to proprietary licenses, the Recipient shall provide each of those licenses and incorporate those licenses in a delivered file.

4. 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 DHS or third-party servers. This attribute must be an aspect of the software's underlying design.

5. 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 underling design.

6. 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 is capable of serving 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. PROGRAM INCOME

1. Post-award program income:

a. During the performance period of the cooperative agreement, the Recipient is authorized to add program income to the funds awarded by DHS and use the program income under the same terms and conditions of this agreement. Program income for the Recipient shall be defined as the gross income received by the recipient, directly generated by the cooperative agreement award or earned during the period of the award. Program income includes, but is not limited to, fees charged for membership, managed security services, entity characterizations and analysis, or other activities when the costs for the activity is charged to this agreement.

b. It is the recipient's responsibility to identify, document and record the income generated. Consistent with the policy and processes outlined in 2 C.F. R. §200.307, pertinent guidance and options, this award will be subject to the additive method for identifying and recording program income. Under this method, any program income earned shall be used to further existing project objectives and performance metrics. All instances of program income shall be clearly delineated and summarized (including identification of project objectives supported by the program income) in each progress and financial report submission pursuant to the deadlines established in Article I.

M. PUBLICATIONS

1. The Recipient agrees to clearly reference DHS investments in the project during all phases of community outreach outlined in the DHS-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 funding which are submitted for publication in any magazine, journal, or trade paper shall carry the following statement:

Acknowledgement. "This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, (19PDMSI00002)."
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 sub-award made under this Agreement the requirements of this award term (Publications).

2. Enhancing Public Access to Publications. "DHS Policy explicitly recognizes and upholds the principles of copyright. Authors and journals can continue to assert copyright in DHS-funded scientific publications, in accordance with current practice. The policy encourages authors to exercise their right to give DHS a copy of their final manuscript or software before publication. While individual copyright arrangements can take many forms, DHS encourages investigators to sign agreements that specifically allow the manuscript

or software to be deposited with DHS for public posting or use after journal publication. Institutions and investigators may wish to develop particular contract 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 DHS upon acceptance for Journal publication or thereafter, for public access purposes through DHS'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 DHS under this Agreement shall be done only after coordination, in writing between the Recipient and DHS.

b. The Recipient agrees to notify the DHS Project Officer 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

N. SITE VISITS

The DHS, 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 the DHS on the premises of the Recipient, or a contractor under this Award, the Recipient shall provide and shall 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 shall be performed in such a manner that will not unduly delay the work.

O. TRAVEL

Travel required in the performance of the duties approved in this Award must comply with §200.474. **Foreign travel must be approved by DHS 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.

P. PUBLIC HEALTH

Recipient shall ensure, to the extent consistent with law, that any Recipient personnel whose primary duty station is located in a federal facility comply with all public health rules, disclosures, and requirements applicable to Recipient personnel working in such facility.

Q. TERMINATION

Either the Recipient or the DHS may terminate this Award by giving written notice to the other party at least thirty (30) calendar days prior to the effective date of the termination. 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. Closeout of this Award will be commenced and processed pursuant to §200.339.

Non-Renewal of the Cooperative Agreement:
In the event this agreement is not renewed, the awardee agrees to provide for an orderly and efficient

transition, should a successor awardee be selected by DHS.

R. GOVERNING PROVISIONS

The following are incorporated into this Award by this reference:

31 CFR 205	Rules and Procedures for Funds Transfers
2 C.F.R. Part 200	Uniform Administrative Requirement, Cost Principles, and Audit Requirements for Federal Awards
NOFO	DHS-20-CISA-123- ISAC000001
Application	Grant Application and Assurances dated September 2021

S. ORDER OF PRECEDENCE

1. 2 C.F.R. Part 200, "Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards."
2. The terms and conditions of this Award.
