ERIC GARCETTI
MAYOR

January 16, 2019

Honorable Members of the City Council
c/o City Clerk
Room 395, City Hall

Re: Fiscal Year 2018 Los Angeles Cyber Lab "Information Sharing and Analysis Organization Pilot Grant" Sub-Award Acceptance

Dear Honorable Members:

Transmitted herewith, for consideration by the Los Angeles City Council, is a request to accept a subaward of the Fiscal Year 2018 Department of Homeland Security "Los Angeles Cyber Lab - An Internet Security - Information Sharing and Analysis Organization Pilot" Grant (the "ISAO Pilot Grant") on behalf of the City of Los Angeles ("City") in the amount of $150,000. The ISAO Pilot Grant was awarded to the Los Angeles Cyber Lab, Inc. ("LA Cyber Lab") on September 29, 2018 in the amount of $2,992,863. Under the terms of the grant, the Mayor's Office has been designated as a subrecipient of the grant to provide management and administration of the grant on behalf of the LA Cyber Lab.

BACKGROUND

The Los Angeles Cyber Lab

In August 2017, the Mayor announced the launch of the LA Cyber Lab, the nation's first regional public-private partnership for cybersecurity information sharing. It is a California non-profit public benefit corporation dedicated to protecting Los Angeles

residents and businesses from malicious cyber threats. Membership is free and open to the public, and currently includes over 500 businesses from a broad cross-section of the LA business community. An advisory board of 30 LA businesses is co-chaired by the Mayor. An independent fiduciary board manages the LA Cyber Lab's daily operations. To date, the LA Cyber Lab has embarked on several important initiatives with the City:

Protection and Alerts—Each day, the City's Information Technology Agency (ITA) Security Team, through its award-winning Integrated Security Operations Center, analyzes more than a billion security-related events traveling across City networks. This critical work helps protect City networks from cyber-attacks, and catches a significant number of threats that are not previously identified. These cyber threats are gathered, combined with threats identified by federal and private sector partners, and shared with LA Cyber Lab members on a daily basis, which they can use to protect their own computer systems.

No other major city makes its threat intelligence data freely and publicly available to help protect its residents. This has established LA as a national leader in municipal cybersecurity and demonstrates its commitment to treating the online safety of its residents as part of its public safety mission.

Last year, the LA Cyber lab began also receiving threats identified by private sector partners, which are in turn shared with the City to help bolster its defenses. Eventually, the LA Cyber Lab will build a central platform, through which the City and the business community can help each other identify potential cyber-attacks in real-time, enhancing everyone's internal security protections.

Public Engagement— The LA Cyber Lab is also facilitating and promoting innovation and education to protect LA's residents. It has begun hosting educational webinars and networking events that help connect law enforcement resources with cutting-edge practitioners in cybersecurity. It is working with academia to provide cybersecurity career training for students and best practices for business executives. In the future, the LA Cyber Lab will create an innovation incubator – a space to allow researchers, startups and developers to test their security tools and to give students an environment to hone skills in a virtual network.

FY 2018 Information Sharing and Analysis Organization Pilot Grant Award
On September 29, 2018, the U.S. Department of Homeland Security ("DHS") awarded the ISAO Pilot Grant to the LA Cyber Lab in the amount of $2,992,863, with grant performance period from September 30, 2018 through September 29, 2019 (Attachment 1). The ISAO Pilot Grant provides funding for expansion of the LA Cyber Lab into a fully functional regionally based information sharing and analysis organization ("ISAO") to develop collaboration between government, higher education, industry and non-profit organizations.

At DHS's request, the Mayor's Office submitted a letter of support with the LA Cyber Lab's grant application indicating its expertise and ability to handle the management and administration requirements of the federal grant award (Attachment 2). The grant award budget approved by DHS and the LA Cyber Lab allocates approximately 5% of the total award - $150,000 - to the City to provide management and administration ("M&A") of the grant on behalf of the LA Cyber Lab (Attachment 3-4).

The grant will require a subrecipient agreement between the LA Cyber Lab and the City of Los Angeles as a subrecipient of its grant allocation. There is no match requirement associated with this grant.

M&A costs shall be allocated towards salary and fringe benefits for the Mayor's Office grant, contract, and fiscal management teams. Grant specialist duties and responsibilities include all grant monitoring and reporting, grant guideline compliance, coordination and communication with DHS and general program management. Attorney/contract specialists shall assist the LA Cyber Lab with the procurement of equipment and services. Fiscal specialists shall ensure the timely, accurate, and appropriate execution of all grant expenditures, reimbursements, and fund draw-downs, as well as preparing and maintaining all necessary documentation to ensure compliance with accepted auditing standards.

RECOMMENDATIONS

It is therefore requested that the City Council:

1. **Authorize** the Mayor, or his designee, to:

    a. Accept, on behalf of the City of Los Angeles, the Fiscal Year 2018 Los Angeles Cyber Lab - An Internet Security - Information Sharing and

Analysis Organization Pilot Grant subaward in the amount of $150,000 for a grant performance period of September 30, 2018 through September 29, 2019 to fund management and administration of the grant on behalf of the LA Cyber Lab, Inc., as outlined above;

b. Negotiate and execute a subaward agreement between the LA Cyber Lab, Inc. and the City of Los Angeles for a term of one year, from September 30, 2018 through September 29, 2019 for receipt of FY18 ISAO Pilot Grant funds, consistent with the approved grant budget and in accordance with the agreement attached to this transmittal, subject to the approval of the City Attorney as to form;

c. Submit to the LA Cyber Lab, Inc., on behalf of the City, requests for drawdown of funds or reimbursements of City funds expended for eligible grant purposes; and

d. Receive, deposit into, and disburse from a new FY 18 ISAO Pilot Grant Fund, the grant funds from the FY 18 ISAO Pilot grant award.

2. **Authorize** the Controller to :

a. Establish a new interest-bearing fund entitled "FY18 ISAO Pilot Grant Fund," and create a receivable in the Fund in the amount of $150,000 for the FY18 ISAO Pilot Grant;

b. Create a receivable in Fund XXX in the amount of $150,000 for the FY 18 ISAO Pilot Grant; and

c. Adopt the FY18 ISAO Pilot Grant and authorize the Mayor to create new appropriation accounts within the FY18 ISAO Pilot Grant Fund No. XXX for the FY18 ISAO Pilot Grant, as follows:

Appropriation Acct No.	Account Name	Amount
46R146	Mayor	$100,415.05
46R299	Reimbursement of General Fund Costs	$49,584.95
	Total:	**$150,000.00**

d. Transfer appropriations within Fund XXX to the General Fund to reimburse the General Fund as follows:

TRANSFER FROM:

Fund/ Dept.	Account	Account Name		Amount
XXX/46	46R146	Mayor		$100,415.05
			TOTAL:	$100,415.05

TRANSFER TO:

Fund/ Dept.	Account	Account Name		Amount
100/46	001020	Grant Reimbursed		$100,415.05
			TOTAL:	$100,415.05

e. Transfer up to $49,584.95 from Fund XXX, Account 46R299 to the General Fund 100/46, Revenue Source 5346, for reimbursement of grant funded fringe benefits; and

f. Transfer cash from Fund XXX/46 to reimburse the General Fund, on an as-needed basis, upon presentation of proper documentation from City Departments, subject to the approval of the Mayor's Office of Public Safety.

3. **Authorize** the Mayor, or designee, to prepare Controller instructions for any technical adjustments, subject to the approval of the City Administrative Officer, and authorize the Controller to implement the instructions.

Sincerely,

ERIC GARCETTI
Mayor

EG:rw

Attachments
1 Award Letter and Amendment No. 1
2 Letter of Support
3 Grant Application Project & Budget Narrative
4 Resolution of the LA Cyber Lab, Inc. Board of Directors

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

Homeland Security

September 29, 2018

Attachment 1

Mr. Jacob M. Finn
Policy Manager
Los Angeles Cyber Lab Inc.
200 North Spring Street, Suite 303
Los Angeles, CA 90012-3239

Re: **DHS Award Number: 18PDSAO00002-01-00**
The Los Angeles Cyber Lab: An Internet Security - Information Sharing and Analysis Organization (IS-ISAO) Pilot

Dear Mr. Finn:

Congratulations! I am pleased to inform you that the Department of Homeland Security (DHS) has approved the Los Angeles Cyber Lab Inc.'s grant application entitled, "The Los Angeles Cyber Lab: An Internet Security - Information Sharing and Analysis Organization(IS-ISAO) Pilot" submitted in response to DHS Notice of Funding Opportunity Number, DHS-18-NPPD-128-ISAO-001.

DHS will award the LA Cyber Lab a total of $2,992,863 for the budget period of 10/01/2018 - 09/30/2019. The full balance is restricted until certification of required training is submitted to DHS, as outlined in the 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 Laura Carlson, Project Officer, at laura.carlson@hq.dhs.gov or (703) 705-6226 on technical/programmatic matters, or Shareef Prater, Grants Officer at shareef.prater@hq.dhs.gov or (202) 447-5903 on administrative matters.

Sincerely,

Shareef Prater
Grants Officer
Grants and Financial Assistance Division
Office of Procurement Operations
Office of the Chief Procurement Officer
Department of Homeland Security

Enclosure(s)

1. DATE ISSUED MM/DD/YYYY	2. CFDA NO.	3. ASSISTANCE TYPE
09/29/2018	97.128	Cooperative Agreement

1a. SUPERSEDES AWARD NOTICE dated
except that any additions or restrictions previously imposed remain in effect unless specifically rescinded

4. GRANT NO.	5. ACTION TYPE
18PDSAO00002-01-00 Formerly	New

6. PROJECT PERIOD	MM/DD/YYYY		MM/DD/YYYY
From	10/01/2018	Through	09/30/2019

7. BUDGET PERIOD	MM/DD/YYYY		MM/DD/YYYY
From	10/01/2018	Through	09/30/2019

Department of Homeland Security

DHS Grants and Financial Assistance Division (GFAD)

245 Murray Lane, SW
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)

Internet Security - Information Sharing and Analysis Organizations (IS-ISAO) Pilot - 2018

9a. GRANTEE NAME AND ADDRESS

Los Angeles Cyber Lab, Inc
200 North Spring Street, Suite 303
Los Angeles, CA 90012-3239

9b. GRANTEE PROJECT DIRECTOR

Mr. Jacob Michael Finn
200 North Spring Street, Suite 303
Los Angeles, CA 90012-3239
Phone: (213) 310-1276

10a. GRANTEE AUTHORIZING OFFICIAL

Mr. Jacob Michael Finn
200 North Spring Street, Suite 303
Los Angeles, CA 90012-3239
Phone: (213) 310-1276

10b. FEDERAL PROJECT OFFICER

Laura Carlson
7th and D Street, SW
Washington, DC 20407
Phone: 703-705-6226

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	0.00
b.	Fringe Benefits	0.00
c.	Total Personnel Costs	0.00
d.	Equipment	1,960,000.00
e.	Supplies	135,000.00
f.	Travel	0.00
g.	Construction	0.00
h.	Other	0.00
i.	Contractual	897,863.00
j.	TOTAL DIRECT COSTS →	2,992,863.00
k.	INDIRECT COSTS	0.00
l.	**TOTAL APPROVED BUDGET**	2,992,863.00
m.	Federal Share	2,992,863.00
n.	Non-Federal Share	0.00

12. AWARD COMPUTATION

a. Amount of Federal Financial Assistance (from item 11m)	2,992,863.00
b. Less Unobligated Balance From Prior Budget Periods	0.00
c. Less Cumulative Prior Award(s) This Budget Period	0.00
d. **AMOUNT OF FINANCIAL ASSISTANCE THIS ACTION**	2,992,863.00
13. Total Federal Funds Awarded to Date for Project Period	2,992,863.00

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. 2		d. 5	
b. 3		e. 6	
c. 4		f. 7	

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)

See Terms and Conditions

GRANTS MANAGEMENT OFFICIAL: **Shareef Prater**

17. OBJ CLASS 4102	18a. VENDOR CODE 831821160	18b. EIN	19. DUNS 081371107	20. CONG. DIST. 34
FY-ACCOUNT NO.	DOCUMENT NO.	ADMINISTRATIVE CODE	AMT ACTION FIN ASST	APPROPRIATION
21. a. CC837080566	b. PDSAO00002A	c. SAO1	d. $2,992,863.00	e. 7080566
22. a.	b.	c.	d.	e.
23. a.	b.	c.	d.	e.

SPECIAL CONDITIONS

1. **All grant funds are restricted until LA Cyber Labs Inc has certified that it has completed training for the Payment Management System. The DHS Grants Officer will provide additional details regarding this restriction.**

AWARD ATTACHMENTS

Los Angeles Cyber Lab, Inc 18PDSAO00002-01-00

1. Terms and Conditions
2. Terms and Conditions Appendix I

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

In addition to the **DHS Standard Terms and Conditions** as outlined here: http://www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions, 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

1. All grant funds are restricted until LA Cyber Lab Inc has certified that it has completed training for the Payment Management System. The Grants Officer will provide additional details regarding this restriction.

2. DHS will require payments as reimbursements. Reimbursement requests must include supporting documentation that the transaction was executed; e.g., bank statement, electronic reference, etc.

3. Performance Metrics should be reported quarterly to measure the effectiveness of IS-ISAC engagement, recruitment and collaboration during the performance period. See Appendix I for more detail.

B. DHS PROGRAMMATIC INVOLVEMENT

1. DHS will exercise substantial programmatic involvement through this cooperative agreement. This includes monitoring project progress; providing technical assistance; disapproving and approving sub-projects, work plans or modifications thereto; holding kickoff meetings; conducting biennial reviews; conducting programmatic reviews; coordinating standards development activities; and coordinating self-certification activities.

2. Coordination/consultation through DHS with other relevant federal departments and agencies is required.

C. AMENDMENTS AND REVISIONS

1. Budget Revisions

a. The Recipient shall obtain prior written approval from the DHS Grants Officer for 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.

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. 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 in order 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. In addition, extension requests shall not be processed without up-to-date performance and financial status reports.

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

D. 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 CFR 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 DHS.

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 due with the Final Progress Report ninety (90) days after the expiration of the Project Period, and shall be submitted via GrantSolutions using the **Grant Note submission** guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

E. FINANCIAL REPORTS

1. Quarterly Federal Financial Reports – the Recipient shall submit a Federal Financial Report (SF-425) to the DHS Grants Officer no later than thirty (30) days after the end of the reporting period end date. Reports are due on 1/31/2019, 4/30/2019, 7/31/2019 and 10/30/2019. The report shall be submitted via GrantSolutions using the FFR submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

2. Final Federal Financial Report – the Recipient shall submit the final Federal Financial Report (SF-425) to the DHS Grants Officer no later than ninety (90) days after the end of the Project Period end date. The report shall be submitted via www.GrantSolutions.gov using the **FFR submission guidance** found here: https://www.grantsolutions.gov/support/granteeUsers.html

3. Quarterly Federal Financial Reports (Cash Transaction) – the Recipient shall submit the Federal Financial Report (SF-425) Cash Transaction Report to the Department of Health and Human Services, Payment Management System. Quarterly Cash Transaction reports shall be submitted no later than 1/30, 4/30, 7/30, and 10/30.

F. PAYMENT

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.

G. PERFORMANCE REPORTS

1. Quarterly Performance Reports – the Recipient shall submit performance reports to the DHS Grants Officer no later than thirty (30) days after the end of the reporting period end date. Reports are due on 1/31/2019, 4/30/2019, 7/31/2019 and 10/30/2019. The report shall be submitted via GrantSolutions using the Grant Note submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

a. Performance reports must provide information on the overall progress by quarter. These reports shall include:

* A comparison of actual accomplishments with the goals and objectives established for the period.
* Reasons why established objectives were not met, if applicable.
* Other pertinent information including, when appropriate, analysis and explanation of cost overruns.

b. If the performance report contains any information that is deemed proprietary, the Recipient will denote the beginning and ending of such information with asterisks (******)

c. For submission of this information, complete the Performance Progress Report (PPR) found at: http://www.fema.gov/media-library/assets/documents/29485 OMB #0970-0334.

2. Final Performance Report – the Recipient shall submit the Final Performance Report to the DHS Grants Officer no later than ninety (90) days after the expiration of the Project Period. The Final Performance Report shall be submitted via GrantSolutions using the Grant Note submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html and please remember to include the program name and grant number in the subject line.

For submission of this information, complete the Performance Progress Report (PPR) found at: http://www.fema.gov/media-library/assets/documents/29485 OMB #0970-0334.

H. PERIOD OF PERFORMANCE

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

1. Acceptable performance of the project 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.

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.

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.

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.

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, as outlined in sections C – G below, for work being performed under this Award.

C. TREATY COMPLIANCE FOR BIOLOGICAL AND CHEMICAL DEFENSE EFFORTS

The Recipient and any Recipient institution shall conduct all biological and chemical defense research, development, and acquisition projects in compliance with all arms control agreements of the U.S., including the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC). DHS Directive 041-01, *Compliance With, and Implementation of, Arms Control Agreements*, requires all such projects to be systematically evaluated for compliance at inception, prior to funding approval, whenever there is significant project change, and whenever in the course of project execution an issue potentially raises a compliance concern.

1. Requirements for Initial Treaty Compliance Review. To ensure compliance with DHS Directive 041-01, for each new biological and/or chemical defense-related effort (including paper and modeling studies) to be conducted under this Award, **the Recipient must submit the following documentation for compliance review and certification prior to funding approval**: a completed Treaty Compliance Form (TCF), which includes a Project Summary; a BWC Checklist; and/or a CWC Checklist.

2. Requirements for Ongoing Treaty Compliance Review. To ensure ongoing treaty compliance for approved biological and/or chemical defense-related efforts funded through this Award, **the Recipient must submit the following documentation for review and approval prior to any significant project change and/or whenever in the course of project execution an issue potentially raises a compliance concern:** an updated Treaty Compliance Form and an updated Statement of Work detailing the proposed modification. The proposed project modification must receive written approval from CAPO prior to initiation. Examples of project modifications include – but are not limited to—the addition of agents, a change in performer, modifications to the scope of work, and changes to the technical approach.

The Recipient should contact the Treaty Compliance Office (TCO) at treatycompliance@hq.dhs.gov to obtain the TCF template, submit the completed Form, or request additional guidance regarding TCO documentation and review requirements, as applicable to (1) new biological and/or chemical defense-related efforts, or (2) modifications to previously approved efforts. The TCO will review all submitted materials and provide written confirmation of approval to initiate work to the Recipient once the treaty compliance certification process is complete. **The Recipient and any Recipient institution shall not initiate any new activities, or execute modifications to approved activities, until receipt of this written confirmation.**

D. REGULATORY COMPLIANCE FOR BIOLOGICAL LABORATORY WORK

The Recipient and any Recipient institution shall conduct all biological laboratory work in compliance with applicable federal regulations; the latest edition of the CDC/NIH Biosafety in Microbiological and Biomedical Laboratories; DHS Directive 066-02, Biosafety; and any local institutional policies that may apply for Recipient institution facilities performing work under this Award. The Regulatory Compliance Office (RCO) will review the submitted Treaty Compliance Form (TCF) for planned work under this Award to determine the applicability of the requirements outlined in this section. **The Recipient must contact the RCO at STregulatorycompliance@hq.dhs.gov for guidance on the requirements, and then submit all required documentation based on RCO guidance, prior to the initiation of any biological laboratory work under this Award.**

1. Requirements for All Biological Laboratory Work. Biological laboratory work includes laboratory activities involving: (1) recombinant DNA or 'rDNA'; (2) Biological Select Agents and Toxins or 'BSAT'; or (3) biological agents, toxins, or other biological materials that are non-rDNA and non-BSAT. **Each Recipient and any Recipient institution to be conducting biological laboratory work under this Award must submit copies of the following documentation, as required by the RCO after review of the TCF(s), for review prior to the initiation of such work:**

a. Research protocol(s), research or project plan(s), or other detailed description of the biological laboratory work to be conducted;
b. Documentation of project-specific biosafety review for biological laboratory work subject to such review in accordance with institutional policy;
c. Institutional or laboratory biosafety manual (may be a related plan or program manual) for each facility/laboratory to be involved in the biological laboratory work;

d. Biosafety training program description (should be provided as available in existing policies, plans, and/or manuals for all relevant facilities/laboratories where work is conducted;

e. Documentation of the most recent safety/biosafety inspection(s) for each facility/laboratory where the biological laboratory work will be conducted;
f. Exposure Control Plan, as applicable;
g. Documentation from the most recent Occupational Safety and Health Administration (OSHA) or State Occupational Safety and Health Agency inspection report; a copy of the OSHA Form 300 Summary of Work Related Injuries and Illnesses or equivalent, for the most recent calendar year; and documentation of any OSHA citations or notices of violation received in the past five years; and

h. Documentation from the most recent U.S. Department of Transportation (DOT) inspection report; and documentation of any DOT citations or notices of violation received in the past five years.

2. Requirements for Research Involving Recombinant DNA (rDNA). Laboratory activities involving rDNA research are defined by the NIH Guidelines for Research Involving Recombinant DNA Molecules, "NIH Guidelines". Each Recipient and any Recipient institution shall conduct all rDNA work in compliance with the NIH Guidelines. In addition to the documentation referenced in Section B.1 above, **each facility conducting research activities involving rDNA under this Award must submit copies of the following documentation to the RCO for review prior to the initiation of such activities:**

a. Institutional Biosafety Committee (IBC) Charter, and/or other available documentation of IBC policies and procedures;
b. Most recent Office of Biotechnology Activities (OBA) acknowledgement letter of the annual IBC Report;
c. IBC-approved rDNA research protocol(s); and
d. Documentation of final IBC approval for each rDNA research protocol and all subsequent renewals and amendments as they occur.

3. Requirements for Activities Involving Biological Select Agents and Toxins (BSAT). **Planned activities involving the possession transfer, and/or use of BSAT must be reviewed by the RCO prior to initiation.** This requirement also applies to activities involving select toxins that fall below the Permissible Toxin Limits, both at facilities registered with the National Select Agent Program and at unregistered facilities. Each Recipient and any Recipient institution shall conduct all BSAT work in compliance with all applicable regulations, including 42 CFR § 73, 7 CFR § 331, and 9 CFR § 121, related entity- and laboratory-specific policies and procedures, and DHS Directive 026-03, *Select Agent and Toxin Security.* **In addition to the documentation referenced in Section B.1 above, each facility conducting activities involving BSAT under this Award must submit copies of the following documentation to the RCO for review prior to the initiation of such activities:**

a. Current APHIS/CDC Certificate of Registration;
b. Most recent APHIS/CDC inspection report(s), response(s), and attachment(s);
c. Current versions of the Biosafety, Security, and Incident Response Plans required and reviewed under the Select Agent Regulations; and

d. Documentation of the most recent annual BSAT facility inspection, as required of the Responsible Official under the Select Agent Regulations.

The Recipient should contact the CAPO at STregulatorycompliance@hq.dhs.gov to obtain the RCO Documentation Request Checklist, submit documentation, or request more information regarding the DHS RCO documentation and compliance review requirements. The CAPO will provide written confirmation of receipt of all required documentation to the designated Point(s) of Contact. The CAPO will evaluate the submitted materials, along with available documentation from any previous reviews for related work at the Recipient and Recipient institution. Additional documentation may be required in some cases and must be submitted upon request. The CAPO will review all submitted materials and provide written confirmation to the Recipient once all requirements have been met.

CAPO review of submitted materials may determine the need for further compliance review requirements, which may include documentation-based and on-site components. The Recipient, and any Recipient institutions conducting biological laboratory work under this Award, must also comply with ongoing CAPO compliance assurance and review requirements, which may include but are not limited to initial and periodic documentation requests, program reviews, site visits, and facility inspections.

The Recipient must promptly report the following to the CAPO, along with any corrective actions taken: (1) any serious or continuing biosafety or BSAT program issues as identified by the APHIS/CDC National Select Agent Program, other compliance oversight authorities, or institutional-level reviews (e.g., IBC or equivalent, laboratory safety/biosafety inspections); (2) any suspension or revocation of the APHIS/CDC Certificate of Registration; and (3) any for-cause suspension or termination of biological, rDNA, or BSAT activities at the laboratories/facilities where DHS-sponsored work is conducted.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to applicable DHS requirements for biological laboratory activities. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., BMBL and NIH Guidelines). The Recipient must provide CAPO documentation sufficient to illustrate this compliance. The CAPO will evaluate compliance measures for these institutions on a case-by-case basis. The Recipient must not initiate work nor provide funds for the conduct of biological laboratory work under this Award without CAPO's formal written approval.

E. RESEARCH INVOLVING ANIMALS

The Recipient and any Recipient institution shall conduct all research involving animals under this Award in compliance with the requirements set forth in the Animal Welfare Act of 1966 (P.L. 89-544), as amended, and the associated regulations in 9 C.F.R., Chapter 1, Subchapter A; the Public Health Service (PHS) Policy on Humane Care and Use of Laboratory Animals (which adopts the "U.S. Government Principles for the Utilization and Care of Vertebrate Animals used in Testing, Research, and Training", 50 FR 20864, May 20, 1985); the National Research Council (NRC) Guide for the Care and Use of Laboratory Animals; the Federation of Animal Science Societies (FASS) Guide for the Care and Use of Agricultural Animals in Agricultural Research and Teaching; and any additional requirements set forth in the DHS Directive for the Care and Use of Animals in Research (026-01). Each Recipient and any Recipient institution planning to perform research involving animals under this Award must comply with the requirements and submit the documentation outlined in this section.

1. Requirements for Initial Review of Research Involving Animals. Research Involving Animals includes any research, experimentation, biological testing, and other related activities involving live, vertebrate animals, including any training for such activities. Each facility conducting research involving animals under this Award must submit copies of the following documentation to the CAPO for review prior to the initiation of such research:

a. Institutional Animal Care and Use Committee (IACUC)-approved animal research protocol(s), including documentation of IACUC approval, any protocol amendments, and related approval notifications;
b. Public Health Service (PHS) Animal Welfare Assurance, including any programmatic amendments, and the most recent NIH Office of Laboratory Animal Welfare (OLAW) approval letter for each Recipient and Recipient institution; OR DHS Animal Welfare Assurance, if the Recipient is not funded by the PHS and does not have a PHS Assurance on file with OLAW. Any affiliated IACUCs must be established under the same requirements as set forth in the PHS Policy;

c. Most recent IACUC semiannual program review and facility inspection reports covering all relevant facilities/laboratories involved in DHS-funded work; and
d. Most recent Association for Assessment and Accreditation of Laboratory Animal Care (AAALAC) inspection report(s) for AAALAC-accredited institution(s) housing and/or performing work involving animals under this Award.

All documentation, as well as any questions or concerns regarding the requirements referenced above, should be submitted to the CAPO at STregulatorycompliance@hq.dhs.gov. Additional documentation may be required in some cases and must be submitted upon request. The CAPO will review all submitted materials and provide written confirmation to the Recipient once all documentation requirements have been met. Upon receipt of this written confirmation, the Recipient may initiate approved animal research projects under this Award, but must address any potential compliance issues or concerns identified by the CAPO. Research involving the use of nonhuman primates or international collaborations involving animal research will require more extensive review prior to approval, and must not begin under this Award without first obtaining a formal certification letter from the CAPO.

The Recipient, as well as any Recipient institution and partner institutions conducting animal research under this Award, shall also comply with ongoing CAPO compliance assurance functions, which may include but are not limited to periodic site visits, program reviews, and facility inspections.

2. Requirements for Ongoing Review of Research Involving Animals. For ongoing animal research activities, each Recipient and any Recipient institutions must submit updates to the CAPO regarding any amendments or changes to (including expiration, renewal, or completion of) ongoing animal protocols as they occur, and may be required to submit annual updates regarding the ACU program at Recipient and Recipient institutions. Annual updates may include, but are not limited to, the IACUC semiannual (program review and facility inspection) reports, the USDA inspection report, and the most recent AAALAC inspection report, as applicable.

The Recipient must promptly report the following to the CAPO, along with any corrective actions taken: (1) any serious or continuing noncompliance with animal care and use regulations and policies adopted by DHS (as referenced above); (2) any change in AAALAC accreditation status; (3) any USDA Notice of Violation; and (4) IACUC suspension of any animal research activity conducted under this Award.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to all DHS requirements for work involving animals. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., Title 9, C.F.R, Chapter 1, Subchapter A; Public Health Service Policy on Humane Care and Use of Laboratory Animals; the Guide for the Care and Use of Laboratory Animals; and the Guide for the Care and Use of Agricultural Animals in Agricultural Research and Teaching). The Recipient must provide CAPO documentation sufficient to illustrate this compliance. The CAPO will evaluate compliance measures for these institutions on a case-by-case basis to determine their sufficiency. The Recipient must not initiate nor provide funds for the conduct of work involving animals at foreign institutions under this Award without formal written approval from the CAPO.

F. REGULATORY REQUIREMENTS FOR LIFE SCIENCES DUAL USE RESEARCH OF CONCERN (DURC)

The Recipient and any Recipient institutions shall conduct all research involving agents and toxins identified in sections III.1 and 6.2.1 of the USG Policy for Oversight of Dual Use Research of Concern and USG Policy for the Institutional Oversight of Dual Use Research of Concern, respectively, in accordance with both policies referenced above and in accordance with any additional requirements set forth in related DHS policies and instructions. Each Recipient and any Recipient institutions planning to perform

1. Requirements for Research Using DURC Agents and Toxins. To ensure compliance with the USG DURC Policies, each facility conducting research involving the agents and toxins identified in sections III.1 and 6.2.1 of the USG DURC Policies under this Award must submit the following documentation for compliance review by CAPO prior to the initiation of such activities.

a. Institutional Review Entity (IRE) charter, and/or other available documentation of IRE policies and procedures, to include the contact information for the Institutional Contact for DURC (ICDUR);

b. Institution's project-specific risk mitigation plan, as applicable;
c. DURC training or education program description;
d. Formal annual assurance of compliance with the USG Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern;
e. A completed iDURC form and a Statement of Work.

2. Required Notifications to DHS:

a. Within 30 calendar days of initial and periodic reviews of institutional review of research with DURC potential, notify CAPO of the results, including whether the research does or does not meet the DURC definition.
b. Report, in writing, any instances of noncompliance and mitigation measures to correct and prevent future instances of noncompliance within 30 calendar days to CAPO.

3. Flowdown Requirements: The Recipient shall include the substance of this section in all sub-awards/contracts at any tier where the sub-Recipient is performing work with agents or toxins identified in sections III.1 of the USG Policy for Oversight of Dual Use Research of Concern and 6.2.1 of the USG Policy for the Institutional Oversight of Dual Use Research of Concern.

The Recipient should contact CAPO at STregulatorycompliance@hq.dhs.gov to submit documentation or to request more information regarding the DHS regulatory documentation and compliance review requirements. CAPO will provide written confirmation of receipt of all required documentation to the designated Points of Contact. CAPO will evaluate the submitted materials. Additional documentation may be required in some cases and must be submitted upon request. CAPO will review all submitted materials and provide written confirmation to the Recipient once all requirements have been met. Upon receipt of this written confirmation, the Recipient may initiate approved projects under this award.

In order to meet the reporting requirements set forth in section IV.2 of the 2012 USG Policy for Oversight of Life Sciences Dual Use Research of Concern (the biannual DURC Data Call), the Recipient and any Recipient institution shall submit documentation regarding all active, planned or recently completed (within twelve months of the submission) unclassified intramural or extramural activities on Federally-funded or conducted life science research projects biannually on the first Monday in May and November. The Recipient should contact
CAPO at STregulatorycompliance@hq.dhs.gov to submit documentation. Documentation should include an update on all listed activities, including status, all agents or toxins incorporated by strain or surrogate name, performers, contract information, and sites of activities. Documentation should also include any changes to existing or completed projects since the most recent submission, including—but not limited to—the addition of agents, a change in performer, modifications to the scope of work, and/or changes to the technical approach. A supplemental report detailing all work involving low pathogenic avian influenza virus H7N9 (LPAI H7N9) and Middle East Respiratory Syndrome Coronavirus (MERS-CoV).

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to the iDURC policy. The Recipient must provide CAPO documentation sufficient to illustrate this compliance. CAPO will evaluate compliance measures for these institutions on a case-by-case basis. The Recipient must not initiate work nor provide funds for the conduct of biological laboratory work under this Award without CAPO's formal written approval.

G. REGULATORY REQUIREMENTS FOR RESEARCH INVOLVING HUMAN SUBJECTS

The Recipient and any Recipient institutions shall conduct all Research Involving Human Subjects in compliance with the requirements set forth in 45 C.F.R. § 46, Subparts A-D, DHS Directive 026-04, Protection of Human Subjects, and any related DHS policies and instructions prior to initiating any work with human subjects under this Award. Each Recipient and any Recipient institutions planning to perform research involving human subjects under this Award must submit the documentation outlined in this section for CAPO review.

1. Requirements for Research Involving Human Subjects. Each facility conducting work involving human subjects under this Award is required to have a project-specific Certification of Compliance letter issued by the CAPO. Each Recipient must submit the following documentation to the CAPO for compliance review and certification prior to initiating research involving human subjects under this Award:

a. Research protocol, as approved by an Institutional Review Board (IRB), for any human subjects research work to be conducted under this Award;
b. IRB approval letter or notification of exemption (see additional information below on exemption determinations), for any human subjects research work to be conducted under this Award;

c. IRB-approved informed consent document(s) (templates) or IRB waiver of informed consent for projects involving human subjects research under this Award; and
d. Federal-wide Assurance (FWA) number from the HHS Office for Human Research Protections (OHRP), or documentation of other relevant assurance, for all Recipient institutions (including Sub-recipients) involved in human subjects research under this Award.

2. Exemptions for Research Involving Human Subjects. Exemption determinations for human subject research to be conducted under this Award should only be made by authorized representatives of (1) an OHRP-registered IRB, or equivalent, or (2) the CAPO. Exemption determinations made by an OHRP-registered IRB, or equivalent, should be submitted to the CAPO for review and record-keeping. Program managers, principal investigators, research staff, and other DHS or institutional personnel should not independently make exemption determinations in the absence of an IRB or CAPO review. DHS program managers (or institutions conducting human subjects' research under this Award) seeking an exemption determination from the CAPO should submit a request to STregulatorycompliance@hq.dhs.gov that includes the following:

a. Research protocol or detailed description of planned activities to be conducted under this Award.

b. Identification of the exemption category that applies to the project(s) to be conducted under this Award and explanation of why the proposed research meets the requirements for that category of exemption.

All documentation, as well as any questions or concerns regarding the requirements referenced above, should be submitted to the CAPO at STregulatorycompliance@hq.dhs.gov. The submitted documentation will be retained by the CAPO and used to conduct a regulatory compliance assessment. Additional documentation may be required in some cases to complete this assessment. The Recipient must provide this documentation upon request, and address in writing any compliance issues or concerns raised by the CAPO before a certification letter is issued and participant enrollment can begin under this Award. The CAPO will review all submitted materials and provide written confirmation to the Recipient once all documentation requirements have been met.

The Recipient and any Recipient institution shall submit updated documentation regarding ongoing research involving human subjects, as available and **prior to the expiration of previous approvals.** Such documentation includes protocol modifications, IRB renewals for ongoing research protocols ("Continuing Reviews"), and notifications of study completion.

The Recipient must promptly report the following to the CAPO, along with any corrective actions taken: (1) any serious or continuing noncompliance with human subjects research regulations and policies adopted by DHS (as referenced above); and (2) suspension, termination, or revocation of IRB approval of any human subjects research activities conducted under this Award.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to all DHS and CAPO requirements for research involving human subjects. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., 45 C.F.R. § 46, including all Subparts, as relevant). The CAPO will evaluate compliance measures for these institutions on a case-by-case basis to determine their sufficiency. The Recipient must not initiate nor provide funds for the conduct of work involving human subjects at foreign institutions under this Contract without formal written approval from the CAPO.

H. 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 CAPO at exportcontrols@hq.dhs.gov.

I. CONTROLLED UNCLASSIFIED INFORMATION

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.

J. PATENT RIGHTS AND DATA RIGHTS

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 http://@hq.dhs.gov.

Data rights.

1. General Requirements. 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:

a. Any data that is first produced under this Award and provided to the Government;
b. Any data owned by third parties that is incorporated in data provided to the Government under this Award; or
c. Any data requested in paragraph 2 below, if incorporated in the Award.

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

2. Additional requirement for this Award.

a. Requirement: 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.

b. Applicability: The requirement in paragraph 2.a of this section applies to any research data that are:

i. Produced under this Award, either as a Recipient or sub-recipient;

ii. Used by the Government in developing an agency action that has the force and effect of law; and

iii. Published, which occurs either when:

1) The research data is published in a peer-reviewed scientific or technical journal; or

2) DHS publicly and officially cites the research data in support of an agency action that has the force and effect of law

c. Definition of "research data:" 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:

1) Preliminary analyses;

2) Drafts of scientific papers;

3) Plans for future research;

4) Peer reviews;

5) Communications with colleagues;

6) Trade secrets;

7) Commercial information;

8) Materials necessary that a researcher must hold confidential until they are published, or similar information which is protected under law; and

9) 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: 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).

K. PROGRAM INCOME

Post-award program income:

In the event program income becomes available to the recipient post-award, it is the recipient's responsibility to notify the DHS Grants Officer to explain how that development occurred, as part of their request for guidance and/or approval. The Grant Officer will review approval requests for program income on a case-by-case basis; approval is not automatic. Consistent with the policy and processes outlined in §200.307, pertinent guidance and options, as determined by the type of recipient and circumstances involved, may be approved by the Grant Officer.

If approval is granted, an award modification will be issued with an explanatory note in the remarks section of the face page, concerning guidance and/or options pertaining to the recipient's approved request. All instances of program income shall be listed in the progress and financial reports.

L. PUBLICATIONS

1. 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:

a. Acknowledgement. "This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, 18PDSAO00002-01-00."

b. 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."

M. 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.

N. 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 2 CFR §200.339.

O. TRAVEL

Travel required in the performance of the duties approved in this Award must comply with 2 CFR § 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 sixty (60) days prior to the commencement of travel.

P. 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. 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.

3. 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 DBS 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.
4. 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. All security requirement documents are located at: http://www.dhs.gov/xopnbiz/grants/index.shtm

5. 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 ISPB, or the applicable Federal department or agency, for approval and processing instructions.

DHS Office of Security ISPB contact information:

Telephone: 202-447-5346

Email: DD254AdministrativeSecurity@dhs.Gov

Mail: Department of Homeland Security
Office of the Chief Security Officer
ATTN: ASD/Industrial Security Program Branch
Washington, D.C. 20528

Q. GOVERNING PROVISIONS

The following are incorporated into this Award by this reference:

31 CFR 205	Rules and Procedures for Funds Transfers
2 CFR Part 200	Uniform Administrative Requirement, Cost Principles, and Audit Requirements for Federal Awards
Application	Grant Application and Assurances dated ___9/17/2018_____, as revised ___[DATE]_____

R. 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

3. The Funding Opportunity, ___DHS-18-NPPD-128-ISAO-001_____, __Internet Security - Information Sharing and Analysis Organizations (IS-ISAO) Pilot_____

4. Application and Assurances dated ___9/17/2018_____, as revised __[DATE]_____

Appendix I - Performance Metrics

Table 1 provides key quarterly performance parameters (KQPP) for measuring the effectiveness of IS-ISAC engagement, recruitment and collaboration during the performance period. Quarterly Performance Metrics must be submitted to the DHS Grants Officer no later than 30 days after the end of each quarter. Reports are due January 31, April 30, July 31 and October 30. The reports shall be submitted via GrantSolutions using the Grant Note submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

Table 1: Project Key Performance Metrics

Performance Measures/Metrics	Performance Objectives	
Measures	Threshold	Objective
Membership		
Number of New members	10-50	50
Number of Individuals Representing Total Membership	10-50	50
Number of State Government members	5-10	10
Number of Local Government Members	5-10	10
Number of Tribal Members	4-6	6
Number of Territorial Members	4-6	6
Number of Fusion Members	4-6	6
Number of Other Members	4-6	6
Average monthly growth rate	1-2%	2%
Stakeholder Engagement		
Number of outreach (conference or event) presentations	2-4	4
Number of cybersecurity tool training events	1-2	2
Number of Analyst to Analyst Membership Exchanges	2-4	4
Number of Membership Online Teleconference Calls	2-4	4

Number of Situational Awareness Room Events	1-2	2
Attendance at Analyst to Analyst Exchange	45-85%	50%
Attendance at Membership Online Conferences	45-85%	50%
IS-ISAC Product Satisfaction	75%-100%	90%
IS-ISAC Services Satisfaction	75%-100%	90%
IS-ISAC Customer Service Satisfaction	75%-100%	90%

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

In addition to the **DHS Standard Terms and Conditions** as outlined here: http://www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions, 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

1. All grant funds are restricted until LA Cyber Labs Inc has certified that it has completed training for the Payment Management System. The Grants Officer will provide additional details regarding this restriction.

2. DHS will require payments as reimbursements. Reimbursement requests must include supporting documentation that the transaction was executed; e.g., bank statement, electronic reference, etc.

3. Performance Metrics should be reported quarterly to measure the effectiveness of IS-ISAC engagement, recruitment and collaboration during the performance period. See Appendix I for more detail.

B. DHS PROGRAMMATIC INVOLVEMENT

1. DHS will exercise substantial programmatic involvement through this cooperative agreement. This includes monitoring project progress; providing technical assistance; disapproving and approving sub-projects, work plans or modifications thereto; holding kickoff meetings; conducting biennial reviews; conducting programmatic reviews; coordinating standards development activities; and coordinating self-certification activities.

2. Coordination/consultation through DHS with other relevant federal departments and agencies is required.

C. AMENDMENTS AND REVISIONS

1. Budget Revisions

a. The Recipient shall obtain prior written approval from the DHS Grants Officer for 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.

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. 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 in order 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. In addition, extension requests shall not be processed without up-to-date performance and financial status reports.

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

D. 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 CFR 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 DHS.

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 due with the Final Progress Report ninety (90) days after the expiration of the Project Period, and shall be submitted via GrantSolutions using the **Grant Note submission** guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

E. FINANCIAL REPORTS

1. Quarterly Federal Financial Reports – the Recipient shall submit a Federal Financial Report (SF-425) to the DHS Grants Officer no later than thirty (30) days after the end of the reporting period end date. Reports are due on 1/31/2019, 4/30/2019, 7/31/2019 and 10/30/2019. The report shall be submitted via GrantSolutions using the FFR submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

2. Final Federal Financial Report – the Recipient shall submit the final Federal Financial Report (SF-425) to the DHS Grants Officer no later than ninety (90) days after the end of the Project Period end date. The report shall be submitted via www.GrantSolutions.gov using the **FFR submission guidance** found here: https://www.grantsolutions.gov/support/granteeUsers.html

3. Quarterly Federal Financial Reports (Cash Transaction) – the Recipient shall submit the Federal Financial Report (SF-425) Cash Transaction Report to the Department of Health and Human Services, Payment Management System. Quarterly Cash Transaction reports shall be submitted no later than 1/30, 4/30, 7/30, and 10/30.

F. PAYMENT

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.

G. PERFORMANCE REPORTS

1. Quarterly Performance Reports – the Recipient shall submit performance reports to the DHS Grants Officer no later than thirty (30) days after the end of the reporting period end date. Reports are due on 1/31/2019, 4/30/2019, 7/31/2019 and 10/30/2019. The report shall be submitted via GrantSolutions using the Grant Note submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

a. Performance reports must provide information on the overall progress by quarter. These reports shall include:

* A comparison of actual accomplishments with the goals and objectives established for the period.
* Reasons why established objectives were not met, if applicable.
* Other pertinent information including, when appropriate, analysis and explanation of cost overruns.

b. If the performance report contains any information that is deemed proprietary, the Recipient will denote the beginning and ending of such information with asterisks (******)

c. For submission of this information, complete the Performance Progress Report (PPR) found at: http://www.fema.gov/media-library/assets/documents/29485 OMB #0970-0334.

2. Final Performance Report – the Recipient shall submit the Final Performance Report to the DHS Grants Officer no later than ninety (90) days after the expiration of the Project Period. The Final Performance Report shall be submitted via GrantSolutions using the Grant Note submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html and please remember to include the program name and grant number in the subject line.

For submission of this information, complete the Performance Progress Report (PPR) found at: http://www.fema.gov/media-library/assets/documents/29485 OMB #0970-0334.

H. PERIOD OF PERFORMANCE

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

1. Acceptable performance of the project 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.

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.

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.

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.

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, as outlined in sections C – G below, for work being performed under this Award.

C. TREATY COMPLIANCE FOR BIOLOGICAL AND CHEMICAL DEFENSE EFFORTS

The Recipient and any Recipient institution shall conduct all biological and chemical defense research, development, and acquisition projects in compliance with all arms control agreements of the U.S., including the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC). DHS Directive 041-01, *Compliance With, and Implementation of, Arms Control Agreements* , requires all such projects to be systematically evaluated for compliance at inception, prior to funding approval, whenever there is significant project change, and whenever in the course of project execution an issue potentially raises a compliance concern.

1. Requirements for Initial Treaty Compliance Review. To ensure compliance with DHS Directive 041-01, for each new biological and/or chemical defense-related effort (including paper and modeling studies) to be conducted under this Award, **the Recipient must submit the following documentation for compliance review and certification prior to funding approval**: a completed Treaty Compliance Form (TCF), which includes a Project Summary; a BWC Checklist; and/or a CWC Checklist.

2. Requirements for Ongoing Treaty Compliance Review. To ensure ongoing treaty compliance for approved biological and/or chemical defense-related efforts funded through this Award, **the Recipient must submit the following documentation for review and approval prior to any significant project change and/or whenever in the course of project execution an issue potentially raises a compliance concern:** an updated Treaty Compliance Form and an updated Statement of Work detailing the proposed modification. The proposed project modification must receive written approval from CAPO prior to initiation. Examples of project modifications include – but are not limited to—the addition of agents, a change in performer, modifications to the scope of work, and changes to the technical approach.

The Recipient should contact the Treaty Compliance Office (TCO) at treatycompliance@hq.dhs.gov to obtain the TCF template, submit the completed Form, or request additional guidance regarding TCO documentation and review requirements, as applicable to (1) new biological and/or chemical defense-related efforts, or (2) modifications to previously approved efforts. The TCO will review all submitted materials and provide written confirmation of approval to initiate work to the Recipient once the treaty compliance certification process is complete. **The Recipient and any Recipient institution shall not initiate any new activities, or execute modifications to approved activities, until receipt of this written confirmation.**

D. REGULATORY COMPLIANCE FOR BIOLOGICAL LABORATORY WORK

The Recipient and any Recipient institution shall conduct all biological laboratory work in compliance with applicable federal regulations; the latest edition of the CDC/NIH Biosafety in Microbiological and Biomedical Laboratories; DHS Directive 066-02, Biosafety; and any local institutional policies that may apply for Recipient institution facilities performing work under this Award. The Regulatory Compliance Office (RCO) will review the submitted Treaty Compliance Form (TCF) for planned work under this Award to determine the applicability of the requirements outlined in this section. **The Recipient must contact the RCO at STregulatorycompliance@hq.dhs.gov for guidance on the requirements, and then submit all required documentation based on RCO guidance, prior to the initiation of any biological laboratory work under this Award.**

1. Requirements for All Biological Laboratory Work. Biological laboratory work includes laboratory activities involving: (1) recombinant DNA or 'rDNA'; (2) Biological Select Agents and Toxins or 'BSAT'; or (3) biological agents, toxins, or other biological materials that are non-rDNA and non-BSAT. **Each Recipient and any Recipient institution to be conducting biological laboratory work under this Award must submit copies of the following documentation, as required by the RCO after review of the TCF(s), for review prior to the initiation of such work:**

a. Research protocol(s), research or project plan(s), or other detailed description of the biological laboratory work to be conducted;
b. Documentation of project-specific biosafety review for biological laboratory work subject to such review in accordance with institutional policy;
c. Institutional or laboratory biosafety manual (may be a related plan or program manual) for each facility/laboratory to be involved in the biological laboratory work;

d. Biosafety training program description (should be provided as available in existing policies, plans, and/or manuals for all relevant facilities/laboratories where work is conducted;

e. Documentation of the most recent safety/biosafety inspection(s) for each facility/laboratory where the biological laboratory work will be conducted;
f. Exposure Control Plan, as applicable;
g. Documentation from the most recent Occupational Safety and Health Administration (OSHA) or State Occupational Safety and Health Agency inspection report; a copy of the OSHA Form 300 Summary of Work Related Injuries and Illnesses or equivalent, for the most recent calendar year; and documentation of any OSHA citations or notices of violation received in the past five years; and

h. Documentation from the most recent U.S. Department of Transportation (DOT) inspection report; and documentation of any DOT citations or notices of violation received in the past five years.

2. Requirements for Research Involving Recombinant DNA (rDNA). Laboratory activities involving rDNA research are defined by the NIH Guidelines for Research Involving Recombinant DNA Molecules, "NIH Guidelines". Each Recipient and any Recipient institution shall conduct all rDNA work in compliance with the NIH Guidelines. In addition to the documentation referenced in Section B.1 above, **each facility conducting research activities involving rDNA under this Award must submit copies of the following documentation to the RCO for review prior to the initiation of such activities:**

a. Institutional Biosafety Committee (IBC) Charter, and/or other available documentation of IBC policies and procedures;
b. Most recent Office of Biotechnology Activities (OBA) acknowledgement letter of the annual IBC Report;
c. IBC-approved rDNA research protocol(s); and
d. Documentation of final IBC approval for each rDNA research protocol and all subsequent renewals and amendments as they occur.

3. Requirements for Activities Involving Biological Select Agents and Toxins (BSAT). **Planned activities involving the possession transfer, and/or use of BSAT must be reviewed by the RCO prior to initiation.** This requirement also applies to activities involving select toxins that fall below the Permissible Toxin Limits, both at facilities registered with the National Select Agent Program and at unregistered facilities. Each Recipient and any Recipient institution shall conduct all BSAT work in compliance with all applicable regulations, including 42 CFR § 73, 7 CFR § 331, and 9 CFR § 121, related entity- and laboratory-specific policies and procedures, and DHS Directive 026-03, *Select Agent and Toxin Security.* **In addition to the documentation referenced in Section B.1 above, each facility conducting activities involving BSAT under this Award must submit copies of the following documentation to the RCO for review prior to the initiation of such activities:**

a. Current APHIS/CDC Certificate of Registration;
b. Most recent APHIS/CDC inspection report(s), response(s), and attachment(s);
c. Current versions of the Biosafety, Security, and Incident Response Plans required and reviewed under the Select Agent Regulations; and

d. Documentation of the most recent annual BSAT facility inspection, as required of the Responsible Official under the Select Agent Regulations.

The Recipient should contact the CAPO at STregulatorycompliance@hq.dhs.gov to obtain the RCO Documentation Request Checklist, submit documentation, or request more information regarding the DHS RCO documentation and compliance review requirements. The CAPO will provide written confirmation of receipt of all required documentation to the designated Point(s) of Contact. The CAPO will evaluate the submitted materials, along with available documentation from any previous reviews for related work at the Recipient and Recipient institution. Additional documentation may be required in some cases and must be submitted upon request. The CAPO will review all submitted materials and provide written confirmation to the Recipient once all requirements have been met.

CAPO review of submitted materials may determine the need for further compliance review requirements, which may include documentation-based and on-site components. The Recipient, and any Recipient institutions conducting biological laboratory work under this Award, must also comply with ongoing CAPO compliance assurance and review requirements, which may include but are not limited to initial and periodic documentation requests, program reviews, site visits, and facility inspections.

The Recipient must promptly report the following to the CAPO, along with any corrective actions taken: (1) any serious or continuing biosafety or BSAT program issues as identified by the APHIS/CDC National Select Agent Program, other compliance oversight authorities, or institutional-level reviews (e.g., IBC or equivalent, laboratory safety/biosafety inspections); (2) any suspension or revocation of the APHIS/CDC Certificate of Registration; and (3) any for-cause suspension or termination of biological, rDNA, or BSAT activities at the laboratories/facilities where DHS-sponsored work is conducted.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to applicable DHS requirements for biological laboratory activities. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., BMBL and NIH Guidelines). The Recipient must provide CAPO documentation sufficient to illustrate this compliance. The CAPO will evaluate compliance measures for these institutions on a case-by-case basis. The Recipient must not initiate work nor provide funds for the conduct of biological laboratory work under this Award without CAPO's formal written approval.

E. RESEARCH INVOLVING ANIMALS

The Recipient and any Recipient institution shall conduct all research involving animals under this Award in compliance with the requirements set forth in the Animal Welfare Act of 1966 (P.L. 89-544), as amended, and the associated regulations in 9 C.F.R., Chapter 1, Subchapter A; the Public Health Service (PHS) Policy on Humane Care and Use of Laboratory Animals (which adopts the "U.S. Government Principles for the Utilization and Care of Vertebrate Animals used in Testing, Research, and Training", 50 FR 20864, May 20, 1985); the National Research Council (NRC) Guide for the Care and Use of Laboratory Animals; the Federation of Animal Science Societies (FASS) Guide for the Care and Use of Agricultural Animals in Agricultural Research and Teaching; and any additional requirements set forth in the DHS Directive for the Care and Use of Animals in Research (026-01). Each Recipient and any Recipient institution planning to perform research involving animals under this Award must comply with the requirements and submit the documentation outlined in this section.

1. Requirements for Initial Review of Research Involving Animals. Research Involving Animals includes any research, experimentation, biological testing, and other related activities involving live, vertebrate animals, including any training for such activities. Each facility conducting research involving animals under this Award must submit copies of the following documentation to the CAPO for review prior to the initiation of such research:

a. Institutional Animal Care and Use Committee (IACUC)-approved animal research protocol(s), including documentation of IACUC approval, any protocol amendments, and related approval notifications;
b. Public Health Service (PHS) Animal Welfare Assurance, including any programmatic amendments, and the most recent NIH Office of Laboratory Animal Welfare (OLAW) approval letter for each Recipient and Recipient institution; OR DHS Animal Welfare Assurance, if the Recipient is not funded by the PHS and does not have a PHS Assurance on file with OLAW. Any affiliated IACUCs must be established under the same requirements as set forth in the PHS Policy;

c. Most recent IACUC semiannual program review and facility inspection reports covering all relevant facilities/laboratories involved in DHS-funded work; and
d. Most recent Association for Assessment and Accreditation of Laboratory Animal Care (AAALAC) inspection report(s) for AAALAC-accredited institution(s) housing and/or performing work involving animals under this Award.

All documentation, as well as any questions or concerns regarding the requirements referenced above, should be submitted to the CAPO at STregulatorycompliance@hq.dhs.gov. Additional documentation may be required in some cases and must be submitted upon request. The CAPO will review all submitted materials and provide written confirmation to the Recipient once all documentation requirements have been met. Upon receipt of this written confirmation, the Recipient may initiate approved animal research projects under this Award, but must address any potential compliance issues or concerns identified by the CAPO. Research involving the use of nonhuman primates or international collaborations involving animal research will require more extensive review prior to approval, and must not begin under this Award without first obtaining a formal certification letter from the CAPO.

The Recipient, as well as any Recipient institution and partner institutions conducting animal research under this Award, shall also comply with ongoing CAPO compliance assurance functions, which may include but are not limited to periodic site visits, program reviews, and facility inspections.

2. Requirements for Ongoing Review of Research Involving Animals. For ongoing animal research activities, each Recipient and any Recipient institutions must submit updates to the CAPO regarding any amendments or changes to (including expiration, renewal, or completion of) ongoing animal protocols as they occur, and may be required to submit annual updates regarding the ACU program at Recipient and Recipient institutions. Annual updates may include, but are not limited to, the IACUC semiannual (program review and facility inspection) reports, the USDA inspection report, and the most recent AAALAC inspection report, as applicable.

The Recipient must promptly report the following to the CAPO, along with any corrective actions taken: (1) any serious or continuing noncompliance with animal care and use regulations and policies adopted by DHS (as referenced above); (2) any change in AAALAC accreditation status; (3) any USDA Notice of Violation; and (4) IACUC suspension of any animal research activity conducted under this Award.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to all DHS requirements for work involving animals. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., Title 9, C.F.R, Chapter 1, Subchapter A; Public Health Service Policy on Humane Care and Use of Laboratory Animals; the Guide for the Care and Use of Laboratory Animals; and the Guide for the Care and Use of Agricultural Animals in Agricultural Research and Teaching). The Recipient must provide CAPO documentation sufficient to illustrate this compliance. The CAPO will evaluate compliance measures for these institutions on a case-by-case basis to determine their sufficiency. The Recipient must not initiate nor provide funds for the conduct of work involving animals at foreign institutions under this Award without formal written approval from the CAPO.

F. REGULATORY REQUIREMENTS FOR LIFE SCIENCES DUAL USE RESEARCH OF CONCERN (DURC)

The Recipient and any Recipient institutions shall conduct all research involving agents and toxins identified in sections III.1 and 6.2.1 of the USG Policy for Oversight of Dual Use Research of Concern and USG Policy for the Institutional Oversight of Dual Use Research of Concern, respectively, in accordance with both policies referenced above and in accordance with any additional requirements set forth in related DHS policies and instructions. Each Recipient and any Recipient institutions planning to perform

1. Requirements for Research Using DURC Agents and Toxins. To ensure compliance with the USG DURC Policies, each facility conducting research involving the agents and toxins identified in sections III.1 and 6.2.1 of the USG DURC Policies under this Award must submit the following documentation for compliance review by CAPO prior to the initiation of such activities.

a. Institutional Review Entity (IRE) charter, and/or other available documentation of IRE policies and procedures, to include the contact information for the Institutional Contact for DURC (ICDUR);

b. Institution's project-specific risk mitigation plan, as applicable;
c. DURC training or education program description;
d. Formal annual assurance of compliance with the USG Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern;
e. A completed iDURC form and a Statement of Work.

2. Required Notifications to DHS:

a. Within 30 calendar days of initial and periodic reviews of institutional review of research with DURC potential, notify CAPO of the results, including whether the research does or does not meet the DURC definition.
b. Report, in writing, any instances of noncompliance and mitigation measures to correct and prevent future instances of noncompliance within 30 calendar days to CAPO.

3. Flowdown Requirements: The Recipient shall include the substance of this section in all sub-awards/contracts at any tier where the sub-Recipient is performing work with agents or toxins identified in sections III.1 of the USG Policy for Oversight of Dual Use Research of Concern and 6.2.1 of the USG Policy for the Institutional Oversight of Dual Use Research of Concern.

The Recipient should contact CAPO at STregulatorycompliance@hq.dhs.gov to submit documentation or to request more information regarding the DHS regulatory documentation and compliance review requirements. CAPO will provide written confirmation of receipt of all required documentation to the designated Points of Contact. CAPO will evaluate the submitted materials. Additional documentation may be required in some cases and must be submitted upon request. CAPO will review all submitted materials and provide written confirmation to the Recipient once all requirements have been met. Upon receipt of this written confirmation, the Recipient may initiate approved projects under this award.

In order to meet the reporting requirements set forth in section IV.2 of the 2012 USG Policy for Oversight of Life Sciences Dual Use Research of Concern (the biannual DURC Data Call), the Recipient and any Recipient institution shall submit documentation regarding all active, planned or recently completed (within twelve months of the submission) unclassified intramural or extramural activities on Federally-funded or conducted life science research projects biannually on the first Monday in May and November. The Recipient should contact
CAPO at STregulatorycompliance@hq.dhs.gov to submit documentation. Documentation should include an update on all listed activities, including status, all agents or toxins incorporated by strain or surrogate name, performers, contract information, and sites of activities. Documentation should also include any changes to existing or completed projects since the most recent submission, including—but not limited to—the addition of agents, a change in performer, modifications to the scope of work, and/or changes to the technical approach. A supplemental report detailing all work involving low pathogenic avian influenza virus H7N9 (LPAI H7N9) and Middle East Respiratory Syndrome Coronavirus (MERS-CoV).

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to the iDURC policy. The Recipient must provide CAPO documentation sufficient to illustrate this compliance. CAPO will evaluate compliance measures for these institutions on a case-by-case basis. The Recipient must not initiate work nor provide funds for the conduct of biological laboratory work under this Award without CAPO's formal written approval.

G. REGULATORY REQUIREMENTS FOR RESEARCH INVOLVING HUMAN SUBJECTS

The Recipient and any Recipient institutions shall conduct all Research Involving Human Subjects in compliance with the requirements set forth in 45 C.F.R. § 46, Subparts A-D, DHS Directive 026-04, Protection of Human Subjects, and any related DHS policies and instructions prior to initiating any work with human subjects under this Award. Each Recipient and any Recipient institutions planning to perform research involving human subjects under this Award must submit the documentation outlined in this section for CAPO review.

1. Requirements for Research Involving Human Subjects. Each facility conducting work involving human subjects under this Award is required to have a project-specific Certification of Compliance letter issued by the CAPO. Each Recipient must submit the following documentation to the CAPO for compliance review and certification prior to initiating research involving human subjects under this Award:

a. Research protocol, as approved by an Institutional Review Board (IRB), for any human subjects research work to be conducted under this Award;
b. IRB approval letter or notification of exemption (see additional information below on exemption determinations), for any human subjects research work to be conducted under this Award;

c. IRB-approved informed consent document(s) (templates) or IRB waiver of informed consent for projects involving human subjects research under this Award; and
d. Federal-wide Assurance (FWA) number from the HHS Office for Human Research Protections (OHRP), or documentation of other relevant assurance, for all Recipient institutions (including Sub-recipients) involved in human subjects research under this Award.

2. Exemptions for Research Involving Human Subjects. Exemption determinations for human subject research to be conducted under this Award should only be made by authorized representatives of (1) an OHRP-registered IRB, or equivalent, or (2) the CAPO. Exemption determinations made by an OHRP-registered IRB, or equivalent, should be submitted to the CAPO for review and record-keeping. Program managers, principal investigators, research staff, and other DHS or institutional personnel should not independently make exemption determinations in the absence of an IRB or CAPO review. DHS program managers (or institutions conducting human subjects' research under this Award) seeking an exemption determination from the CAPO should submit a request to STregulatorycompliance@hq.dhs.gov that includes the following:

a. Research protocol or detailed description of planned activities to be conducted under this Award.

b. Identification of the exemption category that applies to the project(s) to be conducted under this Award and explanation of why the proposed research meets the requirements for that category of exemption.

All documentation, as well as any questions or concerns regarding the requirements referenced above, should be submitted to the CAPO at STregulatorycompliance@hq.dhs.gov. The submitted documentation will be retained by the CAPO and used to conduct a regulatory compliance assessment. Additional documentation may be required in some cases to complete this assessment. The Recipient must provide this documentation upon request, and address in writing any compliance issues or concerns raised by the CAPO before a certification letter is issued and participant enrollment can begin under this Award. The CAPO will review all submitted materials and provide written confirmation to the Recipient once all documentation requirements have been met.

The Recipient and any Recipient institution shall submit updated documentation regarding ongoing research involving human subjects, as available and **prior to the expiration of previous approvals.** Such documentation includes protocol modifications, IRB renewals for ongoing research protocols ("Continuing Reviews"), and notifications of study completion.

The Recipient must promptly report the following to the CAPO, along with any corrective actions taken: (1) any serious or continuing noncompliance with human subjects research regulations and policies adopted by DHS (as referenced above); and (2) suspension, termination, or revocation of IRB approval of any human subjects research activities conducted under this Award.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to all DHS and CAPO requirements for research involving human subjects. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., 45 C.F.R. § 46, including all Subparts, as relevant). The CAPO will evaluate compliance measures for these institutions on a case-by-case basis to determine their sufficiency. The Recipient must not initiate nor provide funds for the conduct of work involving human subjects at foreign institutions under this Contract without formal written approval from the CAPO.

H. 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 CAPO at exportcontrols@hq.dhs.gov.

I. CONTROLLED UNCLASSIFIED INFORMATION

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.

J. PATENT RIGHTS AND DATA RIGHTS

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 http://@hq.dhs.gov.

Data rights.

1. General Requirements. 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:

a. Any data that is first produced under this Award and provided to the Government;
b. Any data owned by third parties that is incorporated in data provided to the Government under this Award; or
c. Any data requested in paragraph 2 below, if incorporated in the Award.

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

2. Additional requirement for this Award.

a. Requirement: 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.

b. Applicability: The requirement in paragraph 2.a of this section applies to any research data that are:

i. Produced under this Award, either as a Recipient or sub-recipient;

ii. Used by the Government in developing an agency action that has the force and effect of law; and

iii. Published, which occurs either when:

1) The research data is published in a peer-reviewed scientific or technical journal; or

2) DHS publicly and officially cites the research data in support of an agency action that has the force and effect of law

c. Definition of "research data:" 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:

1) Preliminary analyses;

2) Drafts of scientific papers;

3) Plans for future research;

4) Peer reviews;

5) Communications with colleagues;

6) Trade secrets;

7) Commercial information;

8) Materials necessary that a researcher must hold confidential until they are published, or similar information which is protected under law; and

9) 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: 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).

K. PROGRAM INCOME

Post-award program income:

In the event program income becomes available to the recipient post-award, it is the recipient's responsibility to notify the DHS Grants Officer to explain how that development occurred, as part of their request for guidance and/or approval. The Grant Officer will review approval requests for program income on a case-by-case basis; approval is not automatic. Consistent with the policy and processes outlined in §200.307, pertinent guidance and options, as determined by the type of recipient and circumstances involved, may be approved by the Grant Officer.

If approval is granted, an award modification will be issued with an explanatory note in the remarks section of the face page, concerning guidance and/or options pertaining to the recipient's approved request. All instances of program income shall be listed in the progress and financial reports.

L. PUBLICATIONS

1. 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:

a. Acknowledgement. "This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, {insert Award Number as outlined in Item #4 on Notice of Award cover page}."

b. 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."

M. 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.

N. 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 2 CFR §200.339.

O. TRAVEL

Travel required in the performance of the duties approved in this Award must comply with 2 CFR § 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 sixty (60) days prior to the commencement of travel.

P. 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. 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.

3. 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 DBS 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.
4. 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. All security requirement documents are located at: http://www.dhs.gov/xopnbiz/grants/index.shtm

5. 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 ISPB, or the applicable Federal department or agency, for approval and processing instructions.

DHS Office of Security ISPB contact information:

Telephone: 202-447-5346

Email: DD254AdministrativeSecurity@dhs.Gov

Mail: Department of Homeland Security
Office of the Chief Security Officer
ATTN: ASD/Industrial Security Program Branch
Washington, D.C. 20528

Q. GOVERNING PROVISIONS

The following are incorporated into this Award by this reference:

31 CFR 205	Rules and Procedures for Funds Transfers
2 CFR Part 200	Uniform Administrative Requirement, Cost Principles, and Audit Requirements for Federal Awards
Application	Grant Application and Assurances dated ___[DATE]_____, as revised ___[DATE]_____

R. 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

3. The Funding Opportunity, ___DHS-18-NPPD-128-ISAO-001_____, __Internet Security - Information Sharing and Analysis Organizations (IS-ISAO) Pilot_____

4. Application and Assurances dated ___9/17/2018_____, as revised __[DATE]_____

Appendix I - Performance Metrics

Table 1 provides key quarterly performance parameters (KQPP) for measuring the effectiveness of IS-ISAC engagement, recruitment and collaboration during the performance period. Quarterly Performance Metrics must be submitted to the DHS Grants Officer no later than 30 days after the end of each quarter. Reports are due January 31, April 30, July 31 and October 30. The reports shall be submitted via GrantSolutions using the Grant Note submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

Table 1: Project Key Performance Metrics

Performance Measures/Metrics	Performance Objectives	
Measures	Threshold	Objective
Membership		
Number of New members	10-50	50
Number of Individuals Representing Total Membership	10-50	50
Number of State Government members	5-10	10
Number of Local Government Members	5-10	10
Number of Tribal Members	4-6	6
Number of Territorial Members	4-6	6
Number of Fusion Members	4-6	6
Number of Other Members	4-6	6
Average monthly growth rate	1-2%	2%
Stakeholder Engagement		
Number of outreach (conference or event) presentations	2-4	4
Number of cybersecurity tool training events	1-2	2
Number of Analyst to Analyst Membership Exchanges	2-4	4
Number of Membership Online Teleconference Calls	2-4	4

Number of Situational Awareness Room Events	1-2	2
Attendance at Analyst to Analyst Exchange	45-85%	50%
Attendance at Membership Online Conferences	45-85%	50%
IS-ISAC Product Satisfaction	75%-100%	90%
IS-ISAC Services Satisfaction	75%-100%	90%
IS-ISAC Customer Service Satisfaction	75%-100%	90%

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

November 23, 2018

Mr. Jacob M. Finn
Policy Manager
Los Angeles Cyber Lab Inc.
200 North Spring Street, Suite 303
Los Angeles, CA 90012-3239

Re: **DHS Award Number: 18PDSAO00002-01-01**
The Los Angeles Cyber Lab: An Internet Security - Information Sharing and Analysis Organization (IS-ISAO) Pilot

Dear Mr. Finn:

The Department of Homeland Security (DHS) issues Amendment #1, which is based on recent negotiations with LA Cyber Labs Inc. This amendment updates the terms and conditions in Article I. Section A., which specify that grant funding will be made available on a quarterly basis pending the review and approval of budget and budget justifications due to the DHS Grants Officer. Moreover, grant payments will be made in advance, instead of on a reimbursement basis. This amendment also updates the project and budget period dates and changes the DHS Project Officer of Record from Laura Carlson to Shawn Pindell. All other terms and conditions remain in effect.

If any additional assistance is required, please have your staff contact Shawn Pindell, Project Officer, at Shawn.Pindell@hq.dhs.gov or (703) 705-6243 on technical/programmatic matters, or Shareef Prater, Grants Officer at shareef.prater@hq.dhs.gov or (202) 447-5903 on administrative matters.

Sincerely,

Shareef Prater
Grants Officer
Grants and Financial Assistance Division
Office of Procurement Operations
Office of the Chief Procurement Officer
Department of Homeland Security

Enclosure(s)

1. DATE ISSUED *MM/DD/YYYY* 11/23/2018	**1a. SUPERSEDES AWARD NOTICE dated** 09/29/2018 except that any additions or restrictions previously imposed remain in effect unless specifically rescinded
2. CFDA NO. 97.128 - Project Grants	
3. ASSISTANCE TYPE Cooperative Agreement	
4. GRANT NO. 18PDSAO00002-01-01 **Formerly**	**5. TYPE OF AWARD** Other
4a. FAIN 18PDSAO00002	**5a. ACTION TYPE** Post Award Amendment
6. PROJECT PERIOD *MM/DD/YYYY* **From** 09/30/2018	*MM/DD/YYYY* **Through** 09/29/2019
7. BUDGET PERIOD *MM/DD/YYYY* **From** 09/30/2018	*MM/DD/YYYY* **Through** 09/29/2019

Department of Homeland Security

DHS Grants and Financial Assistance Division (GFAD)

245 Murray Lane, SW
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)
Internet Security - Information Sharing and Analysis Organizations (IS-ISAO) Pilot - 2018

9a. GRANTEE NAME AND ADDRESS
LOS ANGELES CYBER LAB INC.
Alternate Name: Los Angeles Cyber Lab, Inc
200 N Spring St Ste 303
Los Angeles, CA 90012-3239

9b. GRANTEE PROJECT DIRECTOR
Mr. Jacob Michael Finn
200 North Spring St Ste 303
Los Angeles, CA 90012-9001
Phone: 21331012769780689

10a. GRANTEE AUTHORIZING OFFICIAL
Mr. Jacob Michael Finn
200 North Spring St Ste 303
Los Angeles, CA 90012-9001
Phone: 21331012769780689

10b. FEDERAL PROJECT OFFICER
Shawn Pindell
7th and D Street, SW
Washington, DC 20407
Phone: 703-705-6243

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		0.00
b. Fringe Benefits		0.00
c. Total Personnel Costs		0.00
d. Equipment		1,960,000.00
e. Supplies		135,000.00
f. Travel		0.00
g. Construction		0.00
h. Other		0.00
i. Contractual		897,863.00
j. TOTAL DIRECT COSTS		2,992,863.00
k. INDIRECT COSTS		0.00
l. **TOTAL APPROVED BUDGET**		2,992,863.00
m. Federal Share		2,992,863.00
n. Non-Federal Share		0.00

12. AWARD COMPUTATION

a. Amount of Federal Financial Assistance (from item 11m)	2,992,863.00
b. Less Unobligated Balance From Prior Budget Periods	0.00
c. Less Cumulative Prior Award(s) This Budget Period	2,992,863.00
d. **AMOUNT OF FINANCIAL ASSISTANCE THIS ACTION**	0.00
13. Total Federal Funds Awarded to Date for Project Period	2,992,863.00

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. 2		d. 5	
b. 3		e. 6	
c. 4		f. 7	

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)
See Updated Terms and Conditions

GRANTS MANAGEMENT OFFICIAL:
Shareef Prater
7th and D Street, SW
Washington DC , DC 20407
Phone: (202)447-5903

17.OBJ CLASS 4102	18a. VENDOR CODE 831821160	18b. EIN 831821160	19. DUNS 081371107	20. CONG. DIST. 34
FY-ACCOUNT NO.	**DOCUMENT NO.**	**ADMINISTRATIVE CODE**	**AMT ACTION FIN ASST**	**APPROPRIATION**
21. a. CC837080566	b. PDSAO00002A	c. SAO1	d. $0.00	e. 7080566
22. a.	b.	c.	d.	e.
23. a.	b.	c.	d.	e.

AWARD ATTACHMENTS

Los Angeles Cyber Lab, Inc 18PDSAO00002-01-01

1. Terms and Conditions
2. Terms and Conditions Appendix I

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

In addition to the **DHS Standard Terms and Conditions** as outlined here: http://www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions, 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

1. The grant funding will be made available in advance on a quarterly basis, pending the review and approval of budget and budget justifications due to the DHS Grants Officer.

2. LA Cyber Labs Inc. is required to complete training for the Payment Management System. The Grants Officer will provide additional details.

3. Performance Metrics should be reported quarterly to measure the effectiveness of IS-ISAC engagement, recruitment and collaboration during the performance period. See Appendix I for more detail.

B. DHS PROGRAMMATIC INVOLVEMENT

1. DHS will exercise substantial programmatic involvement through this cooperative agreement. This includes monitoring project progress; providing technical assistance; disapproving and approving sub-projects, work plans or modifications thereto; holding kickoff meetings; conducting biennial reviews; conducting programmatic reviews; coordinating standards development activities; and coordinating self-certification activities.

2. Coordination/consultation through DHS with other relevant federal departments and agencies is required.

C. AMENDMENTS AND REVISIONS

1. Budget Revisions

a. The Recipient shall obtain prior written approval from the DHS Grants Officer for 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.

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. 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 in order 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. In addition, extension requests shall not be processed without up-to-date performance and financial status reports.

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

D. 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 CFR 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 DHS.

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 due with the Final Progress Report ninety (90) days after the expiration of the Project Period, and shall be submitted via GrantSolutions using the **Grant Note submission** guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

E. FINANCIAL REPORTS

1. Quarterly Federal Financial Reports – the Recipient shall submit a Federal Financial Report (SF-425) to the DHS Grants Officer no later than thirty (30) days after the end of the reporting period end date. Reports are due on 1/31/2019, 4/30/2019, 7/31/2019 and 10/30/2019. The report shall be submitted via GrantSolutions using the FFR submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

2. Final Federal Financial Report – the Recipient shall submit the final Federal Financial Report (SF-425) to the DHS Grants Officer no later than ninety (90) days after the end of the Project Period end date. The report shall be submitted via www.GrantSolutions.gov using the **FFR submission guidance** found here: https://www.grantsolutions.gov/support/granteeUsers.html

3. Quarterly Federal Financial Reports (Cash Transaction) – the Recipient shall submit the Federal Financial Report (SF-425) Cash Transaction Report to the Department of Health and Human Services, Payment Management System. Quarterly Cash Transaction reports shall be submitted no later than 1/30, 4/30, 7/30, and 10/30.

F. PAYMENT

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.

G. PERFORMANCE REPORTS

1. Quarterly Performance Reports – the Recipient shall submit performance reports to the DHS Grants Officer no later than thirty (30) days after the end of the reporting period end date. Reports are due on 1/31/2019, 4/30/2019, 7/31/2019 and 10/30/2019. The report shall be submitted via GrantSolutions using the Grant Note submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

a. Performance reports must provide information on the overall progress by quarter. These reports shall include:

* A comparison of actual accomplishments with the goals and objectives established for the period.
* Reasons why established objectives were not met, if applicable.
* Other pertinent information including, when appropriate, analysis and explanation of cost overruns.

b. If the performance report contains any information that is deemed proprietary, the Recipient will denote the beginning and ending of such information with asterisks (******)

c. For submission of this information, complete the Performance Progress Report (PPR) found at: http://www.fema.gov/media-library/assets/documents/29485 OMB #0970-0334.

2. Final Performance Report – the Recipient shall submit the Final Performance Report to the DHS Grants Officer no later than ninety (90) days after the expiration of the Project Period. The Final Performance Report shall be submitted via GrantSolutions using the Grant Note submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html and please remember to include the program name and grant number in the subject line.

For submission of this information, complete the Performance Progress Report (PPR) found at: http://www.fema.gov/media-library/assets/documents/29485 OMB #0970-0334.

H. PERIOD OF PERFORMANCE

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

1. Acceptable performance of the project 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.

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.

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.

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.

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, as outlined in sections C – G below, for work being performed under this Award.

C. TREATY COMPLIANCE FOR BIOLOGICAL AND CHEMICAL DEFENSE EFFORTS

The Recipient and any Recipient institution shall conduct all biological and chemical defense research, development, and acquisition projects in compliance with all arms control agreements of the U.S., including the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC). DHS Directive 041-01, *Compliance With, and Implementation of, Arms Control Agreements*, requires all such projects to be systematically evaluated for compliance at inception, prior to funding approval, whenever there is significant project change, and whenever in the course of project execution an issue potentially raises a compliance concern.

1. Requirements for Initial Treaty Compliance Review. To ensure compliance with DHS Directive 041-01, for each new biological and/or chemical defense-related effort (including paper and modeling studies) to be conducted under this Award, **the Recipient must submit the following documentation for compliance review and certification prior to funding approval**: a completed Treaty Compliance Form (TCF), which includes a Project Summary; a BWC Checklist; and/or a CWC Checklist.

2. Requirements for Ongoing Treaty Compliance Review. To ensure ongoing treaty compliance for approved biological and/or chemical defense-related efforts funded through this Award, **the Recipient must submit the following documentation for review and approval prior to any significant project change and/or whenever in the course of project execution an issue potentially raises a compliance concern:** an updated Treaty Compliance Form and an updated Statement of Work detailing the proposed modification. The proposed project modification must receive written approval from CAPO prior to initiation. Examples of project modifications include – but are not limited to—the addition of agents, a change in performer, modifications to the scope of work, and changes to the technical approach.

The Recipient should contact the Treaty Compliance Office (TCO) at treatycompliance@hq.dhs.gov to obtain the TCF template, submit the completed Form, or request additional guidance regarding TCO documentation and review requirements, as applicable to (1) new biological and/or chemical defense-related efforts, or (2) modifications to previously approved efforts. The TCO will review all submitted materials and provide written confirmation of approval to initiate work to the Recipient once the treaty compliance certification process is complete. **The Recipient and any Recipient institution shall not initiate any new activities, or execute modifications to approved activities, until receipt of this written confirmation.**

D. REGULATORY COMPLIANCE FOR BIOLOGICAL LABORATORY WORK

The Recipient and any Recipient institution shall conduct all biological laboratory work in compliance with applicable federal regulations; the latest edition of the CDC/NIH Biosafety in Microbiological and Biomedical Laboratories; DHS Directive 066-02, Biosafety; and any local institutional policies that may apply for Recipient institution facilities performing work under this Award. The Regulatory Compliance Office (RCO) will review the submitted Treaty Compliance Form (TCF) for planned work under this Award to determine the applicability of the requirements outlined in this section. **The Recipient must contact the RCO at STregulatorycompliance@hq.dhs.gov for guidance on the requirements, and then submit all required documentation based on RCO guidance, prior to the initiation of any biological laboratory work under this Award.**

1. Requirements for All Biological Laboratory Work. Biological laboratory work includes laboratory activities involving: (1) recombinant DNA or 'rDNA'; (2) Biological Select Agents and Toxins or 'BSAT'; or (3) biological agents, toxins, or other biological materials that are non-rDNA and non-BSAT. **Each Recipient and any Recipient institution to be conducting biological laboratory work under this Award must submit copies of the following documentation, as required by the RCO after review of the TCF(s), for review prior to the initiation of such work:**

a. Research protocol(s), research or project plan(s), or other detailed description of the biological laboratory work to be conducted;
b. Documentation of project-specific biosafety review for biological laboratory work subject to such review in accordance with institutional policy;
c. Institutional or laboratory biosafety manual (may be a related plan or program manual) for each facility/laboratory to be involved in the biological laboratory work;

d. Biosafety training program description (should be provided as available in existing policies, plans, and/or manuals for all relevant facilities/laboratories where work is conducted;

e. Documentation of the most recent safety/biosafety inspection(s) for each facility/laboratory where the biological laboratory work will be conducted;
f. Exposure Control Plan, as applicable;
g. Documentation from the most recent Occupational Safety and Health Administration (OSHA) or State Occupational Safety and Health Agency inspection report; a copy of the OSHA Form 300 Summary of Work Related Injuries and Illnesses or equivalent, for the most recent calendar year; and documentation of any OSHA citations or notices of violation received in the past five years; and

h. Documentation from the most recent U.S. Department of Transportation (DOT) inspection report; and documentation of any DOT citations or notices of violation received in the past five years.

2. Requirements for Research Involving Recombinant DNA (rDNA). Laboratory activities involving rDNA research are defined by the NIH Guidelines for Research Involving Recombinant DNA Molecules, "NIH Guidelines". Each Recipient and any Recipient institution shall conduct all rDNA work in compliance with the NIH Guidelines. In addition to the documentation referenced in Section B.1 above, **each facility conducting research activities involving rDNA under this Award must submit copies of the following documentation to the RCO for review prior to the initiation of such activities:**

a. Institutional Biosafety Committee (IBC) Charter, and/or other available documentation of IBC policies and procedures;
b. Most recent Office of Biotechnology Activities (OBA) acknowledgement letter of the annual IBC Report;
c. IBC-approved rDNA research protocol(s); and
d. Documentation of final IBC approval for each rDNA research protocol and all subsequent renewals and amendments as they occur.

3. Requirements for Activities Involving Biological Select Agents and Toxins (BSAT). **Planned activities involving the possession transfer, and/or use of BSAT must be reviewed by the RCO prior to initiation.** This requirement also applies to activities involving select toxins that fall below the Permissible Toxin Limits, both at facilities registered with the National Select Agent Program and at unregistered facilities. Each Recipient and any Recipient institution shall conduct all BSAT work in compliance with all applicable regulations, including 42 CFR § 73, 7 CFR § 331, and 9 CFR § 121, related entity- and laboratory-specific policies and procedures, and DHS Directive 026-03, *Select Agent and Toxin Security.* **In addition to the documentation referenced in Section B.1 above, each facility conducting activities involving BSAT under this Award must submit copies of the following documentation to the RCO for review prior to the initiation of such activities:**

a. Current APHIS/CDC Certificate of Registration;
b. Most recent APHIS/CDC inspection report(s), response(s), and attachment(s);
c. Current versions of the Biosafety, Security, and Incident Response Plans required and reviewed under the Select Agent Regulations; and

d. Documentation of the most recent annual BSAT facility inspection, as required of the Responsible Official under the Select Agent Regulations.

The Recipient should contact the CAPO at STregulatorycompliance@hq.dhs.gov to obtain the RCO Documentation Request Checklist, submit documentation, or request more information regarding the DHS RCO documentation and compliance review requirements. The CAPO will provide written confirmation of receipt of all required documentation to the designated Point(s) of Contact. The CAPO will evaluate the submitted materials, along with available documentation from any previous reviews for related work at the Recipient and Recipient institution. Additional documentation may be required in some cases and must be submitted upon request. The CAPO will review all submitted materials and provide written confirmation to the Recipient once all requirements have been met.

CAPO review of submitted materials may determine the need for further compliance review requirements, which may include documentation-based and on-site components. The Recipient, and any Recipient institutions conducting biological laboratory work under this Award, must also comply with ongoing CAPO compliance assurance and review requirements, which may include but are not limited to initial and periodic documentation requests, program reviews, site visits, and facility inspections.

The Recipient must promptly report the following to the CAPO, along with any corrective actions taken: (1) any serious or continuing biosafety or BSAT program issues as identified by the APHIS/CDC National Select Agent Program, other compliance oversight authorities, or institutional-level reviews (e.g., IBC or equivalent, laboratory safety/biosafety inspections); (2) any suspension or revocation of the APHIS/CDC Certificate of Registration; and (3) any for-cause suspension or termination of biological, rDNA, or BSAT activities at the laboratories/facilities where DHS-sponsored work is conducted.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to applicable DHS requirements for biological laboratory activities. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., BMBL and NIH Guidelines). The Recipient must provide CAPO documentation sufficient to illustrate this compliance. The CAPO will evaluate compliance measures for these institutions on a case-by-case basis. The Recipient must not initiate work nor provide funds for the conduct of biological laboratory work under this Award without CAPO's formal written approval.

E. RESEARCH INVOLVING ANIMALS

The Recipient and any Recipient institution shall conduct all research involving animals under this Award in compliance with the requirements set forth in the Animal Welfare Act of 1966 (P.L. 89-544), as amended, and the associated regulations in 9 C.F.R., Chapter 1, Subchapter A; the Public Health Service (PHS) Policy on Humane Care and Use of Laboratory Animals (which adopts the "U.S. Government Principles for the Utilization and Care of Vertebrate Animals used in Testing, Research, and Training", 50 FR 20864, May 20, 1985); the National Research Council (NRC) Guide for the Care and Use of Laboratory Animals; the Federation of Animal Science Societies (FASS) Guide for the Care and Use of Agricultural Animals in Agricultural Research and Teaching; and any additional requirements set forth in the DHS Directive for the Care and Use of Animals in Research (026-01). Each Recipient and any Recipient institution planning to perform research involving animals under this Award must comply with the requirements and submit the documentation outlined in this section.

1. Requirements for Initial Review of Research Involving Animals. Research Involving Animals includes any research, experimentation, biological testing, and other related activities involving live, vertebrate animals, including any training for such activities. Each facility conducting research involving animals under this Award must submit copies of the following documentation to the CAPO for review prior to the initiation of such research:

a. Institutional Animal Care and Use Committee (IACUC)-approved animal research protocol(s), including documentation of IACUC approval, any protocol amendments, and related approval notifications;
b. Public Health Service (PHS) Animal Welfare Assurance, including any programmatic amendments, and the most recent NIH Office of Laboratory Animal Welfare (OLAW) approval letter for each Recipient and Recipient institution; OR DHS Animal Welfare Assurance, if the Recipient is not funded by the PHS and does not have a PHS Assurance on file with OLAW. Any affiliated IACUCs must be established under the same requirements as set forth in the PHS Policy;

c. Most recent IACUC semiannual program review and facility inspection reports covering all relevant facilities/laboratories involved in DHS-funded work; and
d. Most recent Association for Assessment and Accreditation of Laboratory Animal Care (AAALAC) inspection report(s) for AAALAC-accredited institution(s) housing and/or performing work involving animals under this Award.

All documentation, as well as any questions or concerns regarding the requirements referenced above, should be submitted to the CAPO at STregulatorycompliance@hq.dhs.gov. Additional documentation may be required in some cases and must be submitted upon request. The CAPO will review all submitted materials and provide written confirmation to the Recipient once all documentation requirements have been met. Upon receipt of this written confirmation, the Recipient may initiate approved animal research projects under this Award, but must address any potential compliance issues or concerns identified by the CAPO. Research involving the use of nonhuman primates or international collaborations involving animal research will require more extensive review prior to approval, and must not begin under this Award without first obtaining a formal certification letter from the CAPO.

The Recipient, as well as any Recipient institution and partner institutions conducting animal research under this Award, shall also comply with ongoing CAPO compliance assurance functions, which may include but are not limited to periodic site visits, program reviews, and facility inspections.

2. Requirements for Ongoing Review of Research Involving Animals. For ongoing animal research activities, each Recipient and any Recipient institutions must submit updates to the CAPO regarding any amendments or changes to (including expiration, renewal, or completion of) ongoing animal protocols as they occur, and may be required to submit annual updates regarding the ACU program at Recipient and Recipient institutions. Annual updates may include, but are not limited to, the IACUC semiannual (program review and facility inspection) reports, the USDA inspection report, and the most recent AAALAC inspection report, as applicable.

The Recipient must promptly report the following to the CAPO, along with any corrective actions taken: (1) any serious or continuing noncompliance with animal care and use regulations and policies adopted by DHS (as referenced above); (2) any change in AAALAC accreditation status; (3) any USDA Notice of Violation; and (4) IACUC suspension of any animal research activity conducted under this Award.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to all DHS requirements for work involving animals. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., Title 9, C.F.R, Chapter 1, Subchapter A; Public Health Service Policy on Humane Care and Use of Laboratory Animals; the Guide for the Care and Use of Laboratory Animals; and the Guide for the Care and Use of Agricultural Animals in Agricultural Research and Teaching). The Recipient must provide CAPO documentation sufficient to illustrate this compliance. The CAPO will evaluate compliance measures for these institutions on a case-by-case basis to determine their sufficiency. The Recipient must not initiate nor provide funds for the conduct of work involving animals at foreign institutions under this Award without formal written approval from the CAPO.

F. REGULATORY REQUIREMENTS FOR LIFE SCIENCES DUAL USE RESEARCH OF CONCERN (DURC)

The Recipient and any Recipient institutions shall conduct all research involving agents and toxins identified in sections III.1 and 6.2.1 of the USG Policy for Oversight of Dual Use Research of Concern and USG Policy for the Institutional Oversight of Dual Use Research of Concern, respectively, in accordance with both policies referenced above and in accordance with any additional requirements set forth in related DHS policies and instructions. Each Recipient and any Recipient institutions planning to perform

1. Requirements for Research Using DURC Agents and Toxins. To ensure compliance with the USG DURC Policies, each facility conducting research involving the agents and toxins identified in sections III.1 and 6.2.1 of the USG DURC Policies under this Award must submit the following documentation for compliance review by CAPO prior to the initiation of such activities.

a. Institutional Review Entity (IRE) charter, and/or other available documentation of IRE policies and procedures, to include the contact information for the Institutional Contact for DURC (ICDUR);

b. Institution's project-specific risk mitigation plan, as applicable;
c. DURC training or education program description;
d. Formal annual assurance of compliance with the USG Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern;
e. A completed iDURC form and a Statement of Work.

2. Required Notifications to DHS:

a. Within 30 calendar days of initial and periodic reviews of institutional review of research with DURC potential, notify CAPO of the results, including whether the research does or does not meet the DURC definition.
b. Report, in writing, any instances of noncompliance and mitigation measures to correct and prevent future instances of noncompliance within 30 calendar days to CAPO.

3. Flowdown Requirements: The Recipient shall include the substance of this section in all sub-awards/contracts at any tier where the sub-Recipient is performing work with agents or toxins identified in sections III.1 of the USG Policy for Oversight of Dual Use Research of Concern and 6.2.1 of the USG Policy for the Institutional Oversight of Dual Use Research of Concern.

The Recipient should contact CAPO at STregulatorycompliance@hq.dhs.gov to submit documentation or to request more information regarding the DHS regulatory documentation and compliance review requirements. CAPO will provide written confirmation of receipt of all required documentation to the designated Points of Contact. CAPO will evaluate the submitted materials. Additional documentation may be required in some cases and must be submitted upon request. CAPO will review all submitted materials and provide written confirmation to the Recipient once all requirements have been met. Upon receipt of this written confirmation, the Recipient may initiate approved projects under this award.

In order to meet the reporting requirements set forth in section IV.2 of the 2012 USG Policy for Oversight of Life Sciences Dual Use Research of Concern (the biannual DURC Data Call), the Recipient and any Recipient institution shall submit documentation regarding all active, planned or recently completed (within twelve months of the submission) unclassified intramural or extramural activities on Federally-funded or conducted life science research projects biannually on the first Monday in May and November. The Recipient should contact
CAPO at STregulatorycompliance@hq.dhs.gov to submit documentation. Documentation should include an update on all listed activities, including status, all agents or toxins incorporated by strain or surrogate name, performers, contract information, and sites of activities. Documentation should also include any changes to existing or completed projects since the most recent submission, including—but not limited to—the addition of agents, a change in performer, modifications to the scope of work, and/or changes to the technical approach. A supplemental report detailing all work involving low pathogenic avian influenza virus H7N9 (LPAI H7N9) and Middle East Respiratory Syndrome Coronavirus (MERS-CoV).

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to the iDURC policy. The Recipient must provide CAPO documentation sufficient to illustrate this compliance. CAPO will evaluate compliance measures for these institutions on a case-by-case basis. The Recipient must not initiate work nor provide funds for the conduct of biological laboratory work under this Award without CAPO's formal written approval.

G. REGULATORY REQUIREMENTS FOR RESEARCH INVOLVING HUMAN SUBJECTS

The Recipient and any Recipient institutions shall conduct all Research Involving Human Subjects in compliance with the requirements set forth in 45 C.F.R. § 46, Subparts A-D, DHS Directive 026-04, Protection of Human Subjects, and any related DHS policies and instructions prior to initiating any work with human subjects under this Award. Each Recipient and any Recipient institutions planning to perform research involving human subjects under this Award must submit the documentation outlined in this section for CAPO review.

1. Requirements for Research Involving Human Subjects. Each facility conducting work involving human subjects under this Award is required to have a project-specific Certification of Compliance letter issued by the CAPO. Each Recipient must submit the following documentation to the CAPO for compliance review and certification prior to initiating research involving human subjects under this Award:

a. Research protocol, as approved by an Institutional Review Board (IRB), for any human subjects research work to be conducted under this Award;
b. IRB approval letter or notification of exemption (see additional information below on exemption determinations), for any human subjects research work to be conducted under this Award;

c. IRB-approved informed consent document(s) (templates) or IRB waiver of informed consent for projects involving human subjects research under this Award; and
d. Federal-wide Assurance (FWA) number from the HHS Office for Human Research Protections (OHRP), or documentation of other relevant assurance, for all Recipient institutions (including Sub-recipients) involved in human subjects research under this Award.

2. Exemptions for Research Involving Human Subjects. Exemption determinations for human subject research to be conducted under this Award should only be made by authorized representatives of (1) an OHRP-registered IRB, or equivalent, or (2) the CAPO. Exemption determinations made by an OHRP-registered IRB, or equivalent, should be submitted to the CAPO for review and record-keeping. Program managers, principal investigators, research staff, and other DHS or institutional personnel should not independently make exemption determinations in the absence of an IRB or CAPO review. DHS program managers (or institutions conducting human subjects' research under this Award) seeking an exemption determination from the CAPO should submit a request to STregulatorycompliance@hq.dhs.gov that includes the following:

a. Research protocol or detailed description of planned activities to be conducted under this Award.

b. Identification of the exemption category that applies to the project(s) to be conducted under this Award and explanation of why the proposed research meets the requirements for that category of exemption.

All documentation, as well as any questions or concerns regarding the requirements referenced above, should be submitted to the CAPO at STregulatorycompliance@hq.dhs.gov. The submitted documentation will be retained by the CAPO and used to conduct a regulatory compliance assessment. Additional documentation may be required in some cases to complete this assessment. The Recipient must provide this documentation upon request, and address in writing any compliance issues or concerns raised by the CAPO before a certification letter is issued and participant enrollment can begin under this Award. The CAPO will review all submitted materials and provide written confirmation to the Recipient once all documentation requirements have been met.

The Recipient and any Recipient institution shall submit updated documentation regarding ongoing research involving human subjects, as available and **prior to the expiration of previous approvals.** Such documentation includes protocol modifications, IRB renewals for ongoing research protocols ("Continuing Reviews"), and notifications of study completion.

The Recipient must promptly report the following to the CAPO, along with any corrective actions taken: (1) any serious or continuing noncompliance with human subjects research regulations and policies adopted by DHS (as referenced above); and (2) suspension, termination, or revocation of IRB approval of any human subjects research activities conducted under this Award.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to all DHS and CAPO requirements for research involving human subjects. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., 45 C.F.R. § 46, including all Subparts, as relevant). The CAPO will evaluate compliance measures for these institutions on a case-by-case basis to determine their sufficiency. The Recipient must not initiate nor provide funds for the conduct of work involving human subjects at foreign institutions under this Contract without formal written approval from the CAPO.

H. 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 CAPO at exportcontrols@hq.dhs.gov.

I. CONTROLLED UNCLASSIFIED INFORMATION

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.

J. PATENT RIGHTS AND DATA RIGHTS

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 http://@hq.dhs.gov.

Data rights.

1. General Requirements. 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:

a. Any data that is first produced under this Award and provided to the Government;
b. Any data owned by third parties that is incorporated in data provided to the Government under this Award; or
c. Any data requested in paragraph 2 below, if incorporated in the Award.

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

2. Additional requirement for this Award.

a. Requirement: 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.

b. Applicability: The requirement in paragraph 2.a of this section applies to any research data that are:

i. Produced under this Award, either as a Recipient or sub-recipient;

ii. Used by the Government in developing an agency action that has the force and effect of law; and

iii. Published, which occurs either when:

1) The research data is published in a peer-reviewed scientific or technical journal; or

2) DHS publicly and officially cites the research data in support of an agency action that has the force and effect of law

c. Definition of "research data:" 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:

1) Preliminary analyses;

2) Drafts of scientific papers;

3) Plans for future research;

4) Peer reviews;

5) Communications with colleagues;

6) Trade secrets;

7) Commercial information;

8) Materials necessary that a researcher must hold confidential until they are published, or similar information which is protected under law; and

9) 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: 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).

K. PROGRAM INCOME

Post-award program income:

In the event program income becomes available to the recipient post-award, it is the recipient's responsibility to notify the DHS Grants Officer to explain how that development occurred, as part of their request for guidance and/or approval. The Grant Officer will review approval requests for program income on a case-by-case basis; approval is not automatic. Consistent with the policy and processes outlined in §200.307, pertinent guidance and options, as determined by the type of recipient and circumstances involved, may be approved by the Grant Officer.

If approval is granted, an award modification will be issued with an explanatory note in the remarks section of the face page, concerning guidance and/or options pertaining to the recipient's approved request. All instances of program income shall be listed in the progress and financial reports.

L. PUBLICATIONS

1. 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:

a. Acknowledgement. "This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, 18PDSAO00002-01-00."

b. 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."

M. 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.

N. 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 2 CFR §200.339.

O. TRAVEL

Travel required in the performance of the duties approved in this Award must comply with 2 CFR § 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 sixty (60) days prior to the commencement of travel.

P. 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. 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.

3. 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 DBS 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.
4. 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. All security requirement documents are located at: http://www.dhs.gov/xopnbiz/grants/index.shtm

5. 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 ISPB, or the applicable Federal department or agency, for approval and processing instructions.

DHS Office of Security ISPB contact information:

Telephone: 202-447-5346

Email: DD254AdministrativeSecurity@dhs.Gov

Mail: Department of Homeland Security
Office of the Chief Security Officer
ATTN: ASD/Industrial Security Program Branch
Washington, D.C. 20528

Q. GOVERNING PROVISIONS

The following are incorporated into this Award by this reference:

31 CFR 205	Rules and Procedures for Funds Transfers
2 CFR Part 200	Uniform Administrative Requirement, Cost Principles, and Audit Requirements for Federal Awards
Application	Grant Application and Assurances dated ___9/17/2018_____, as revised ___[DATE]_____

R. 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

3. The Funding Opportunity, ___DHS-18-NPPD-128-ISAO-001_____, __Internet Security - Information Sharing and Analysis Organizations (IS-ISAO) Pilot_____

4. Application and Assurances dated ___9/17/2018_____, as revised __[DATE]_____

Appendix I - Performance Metrics

Table 1 provides key quarterly performance parameters (KQPP) for measuring the effectiveness of IS-ISAC engagement, recruitment and collaboration during the performance period. Quarterly Performance Metrics must be submitted to the DHS Grants Officer no later than 30 days after the end of each quarter. Reports are due January 31, April 30, July 31 and October 30. The reports shall be submitted via GrantSolutions using the Grant Note submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

Table 1: Project Key Performance Metrics

Performance Measures/Metrics	Performance Objectives	
Measures	Threshold	Objective
Membership		
Number of New members	10-50	50
Number of Individuals Representing Total Membership	10-50	50
Number of State Government members	5-10	10
Number of Local Government Members	5-10	10
Number of Tribal Members	4-6	6
Number of Territorial Members	4-6	6
Number of Fusion Members	4-6	6
Number of Other Members	4-6	6
Average monthly growth rate	1-2%	2%
Stakeholder Engagement		
Number of outreach (conference or event) presentations	2-4	4
Number of cybersecurity tool training events	1-2	2
Number of Analyst to Analyst Membership Exchanges	2-4	4
Number of Membership Online Teleconference Calls	2-4	4

Number of Situational Awareness Room Events	1-2	2
Attendance at Analyst to Analyst Exchange	45-85%	50%
Attendance at Membership Online Conferences	45-85%	50%
IS-ISAC Product Satisfaction	75%-100%	90%
IS-ISAC Services Satisfaction	75%-100%	90%
IS-ISAC Customer Service Satisfaction	75%-100%	90%

ERIC GARCETTI
MAYOR

Attachment 2

September 26, 2018

Shareef Prater, Office of Procurement Operations
U.S. Department of Homeland Security
800 K Street NW, #1000
Washington, DC 20528

Mr. Prater,

This letter responds to your request for a written statement from the City of Los Angeles Mayor's Office of Public Safety regarding our intention to provide fiscal management support for the Los Angeles Cyber Lab, Inc. The Mayor's Office of Public Safety manages and administers millions of dollars each year including security assistance awarded from the Department of Homeland Security (DHS), California Office of Emergency Services, and various non-profit foundations.

It is our understanding that the Los Angeles Cyber Lab, Inc. has applied for DHS assistance under the grant award titled "Internet Security – Information Sharing and Analysis Organizations (IS-ISAO) Pilot" (DHS-18-NPPD-128-ISAO-001). If the Los Angeles Cyber Lab, Inc. is awarded this DHS assistance, the Mayor's Office of Public Safety – Grants, Finance, and Administration Unit is both willing and capable of subcontracting the Management and Administration (M&A) requirements of the award.

Our office will enter into any official agreements and abide by any restrictions as required.

For any additional information, please contact me at jeff.gorell@lacity.org or you may call our office at (213) 978-0677.

Sincerely,

J. F. Gorell

JEFF GORELL
Deputy Mayor, Public Safety

The Los Angeles Cyber Lab

An Internet Security - Information Sharing and Analysis Organization (IS-ISAO) Pilot

DHS-18-NPPD-128-ISAO-001

Project Narrative Submitted By

Los Angeles Cyber Lab Inc.,

A California Nonprofit Public Benefit Corporation

DUNS: 081371107 | EIN: 83-1821160

September 17, 2018

Project Abstract

The Los Angeles Cyber Lab, Inc. (LA Cyber Lab), a California Nonprofit Public Benefit Corporation, seeks to enter into a cooperative agreement with the U.S. Department of Homeland Security to develop and implement a pilot Internet Security - Information Sharing Analysis Organization (IS-ISAO). Leveraging the Cyber Lab's cutting edge solutions, partners, and existing information-sharing arrangements, this cooperative agreement will amplify the online resilience of State, Local, Territorial and Tribal (SLTT) governments by enhancing their capabilities to prepare for, defend against, respond to, and recover from cyber attacks. Funding will allow the Cyber Lab to become a cost-effective, transparent IS-ISAO that can easily be replicated in other risk areas of the United States.

Launched in August 2017, the Los Angeles Cyber Lab is a first of its kind public-private partnership. It is a non-profit organization dedicated to protecting personal and proprietary information from malicious cyber threats by facilitating and promoting innovation, education, and information-sharing between Los Angeles' public and private sectors. The lab is directed and operated by leaders from across all sectors including finance, information technology, healthcare, manufacturing, law, transportation, energy, entertainment, and government. The Cyber Lab's core initiative is the mutual exchange of cyber threat intelligence across private and public sectors, creating collaborative, real-time identification and analysis of threats by the city of Los Angeles, businesses of all sizes, and state and federal partners, including the Department of Homeland Security through the National Cybersecurity & Communications Integration Center. In addition to information-sharing, the Cyber Lab performs widespread outreach activities including offering research and development opportunities for academia, job opportunities for entry-level, career training for professionals, and innovative conferences and events for all customers.

This project expands upon the LA Cyber Lab's three core capabilities. First, the Cyber Lab will build a universal, standardized Threat Intelligence, Analysis, and Sharing Platform (TIASP) which will be accessible to the public at no cost. This will effectively defeat the barrier to machine-to-machine information-sharing between the private sector, SLTT governments, and DHS. Second, the Cyber Lab will build out its personnel and infrastructure. A team of full-time specialized employees will staff the LA Cyber Lab--assuming the current roles of private sector and government volunteers--to ensure the long-term sustainability of the IS-ISAO following the grant's completion. Finally, the lab seeks to expand its stakeholder engagement. Cooperative agreement funds will support annual, monthly, quarterly and other regular conferences, meetings and engagements, and will be used to incubate an IS-ISAO "Cyber Range" that will boost academic and private sector R&D.

I. Purpose and Scope

The Los Angeles Cyber Lab, Inc. seeks to stand up a fully functional Internet Security - Information Sharing Analysis Organization (IS-ISAO) to promote and develop a regional and transnational collaboration of SLTT governments, higher education, industry, and non-profits. The LA Cyber Lab's objectives include: (1) conducting cyber-threat analysis and real-time intelligence sharing; (2) expanding cybersecurity training, education, and workforce development; (3) incubating technological research and development related to cybersecurity and information sharing; and (4) spreading awareness of online best practices.

Funding will enable the Cyber Lab to build out its existing organizational infrastructure, which has already begun the process of providing a public, near real-time cyber information exchange between the public and private sectors. Since founded one year ago, the Cyber Lab has engaged more than 500 small, medium, and large-size businesses in the Los Angeles region, and expanding to establish strategic cross-sector partnerships across the state and nation. The Cyber Lab currently polls Indicators of Compromise (IOCs) from all departments of the City of Los Angeles and multiple large Los Angeles-based private corporations, and pushing those indicators to the National Cybersecurity and Communications Integration Center (NCCIC) through DHS' Automated Information Sharing (AIS) platform. The Cyber Lab shares its IOC reports to the public on a daily basis, helping businesses across the region protect themselves from newly discovered cyber threats. LA Cyber Lab's outreach efforts have effectively engaged hundreds of cybersecurity professionals, students, academics, and policymakers, and have received positive feedback from the community.

This funding proposal expands the LA Cyber Lab's core capabilities through three core strategies. First, it will be used to enhance existing information-sharing technologies and to acquire new technologies that will streamline cyber-threat sharing processes between the IS-ISAO, regional customers, SLTT governments, and the NCCIC. For example, the Cyber Lab will build a universal, standardized Threat Intelligence, Analysis, and Sharing Platform (TIASP) which will be accessible, for free, to private sector companies and SLTT governments. Each endpoint (company or government) will automatically feed threats into the Cyber Lab's (IS-ISAO) TIASP. The threats will be analyzed, correlated, and IOCs distributed back to the feeding customers. Moreover, as previously stated, the ISAO's TIASP will continue to feed real-time threats to the NCCIC through DHS' Automated Information Sharing (AIS) platform using clients such as FLAIR. ***This will directly and effectively eliminate the barriers to information sharing between private companies, SLTT governments, and the Department of Homeland Security***.

Second, the proposal will institutionalize the Cyber Lab with personnel and resources to ensure the long-term sustainability of the IS-ISAO. A Chief Development Officer (CDO) will be engaged to strengthen the LA Cyber Lab's partnerships with the private sector and expand its reach to SLTT across the state of California and to other large cities across the country. The CDO will oversee LA Cyber Lab staff engaged in enhancing the information-sharing platform and outreach and education to the government and business community. Two cyber threat analysts will supplement existing analysts at the Integrated Security Operations Center. Whereas the current analysts are mostly focused on situational awareness and incident handling, the two new threat analysts will be fully dedicated to supporting information-sharing with private sector entities, SLTT governments, and national customers. An IS-ISAO policy specialist will be responsible for overseeing the development of documentation including design, policies and procedures, CONOPS, and operations manuals. The specialist will also be responsible for researching information-sharing best practices and advising/consulting with private sector, SLTT, and federal partners. Finally, a program specialist will be responsible for coordinating the Cyber Lab's annual summit, as well as the regular conferences, cybersecurity training courses, and other outreach events. ***Investments in the Cyber Lab's personnel and infrastructure will directly achieve a fully functional, transparent IS-ISAO with the ability to integrate with other ISACs/ISAOs, SLTT governments, and the Department of Homeland Security.***

The third tier of this proposal builds upon the LA Cyber Lab's commitment to engaging the community and developing the next generation of systems and professionals dedicated to public cybersecurity. The LA Cyber Lab intends to create a real world learning environment--known as the LA Cyber Lab Innovation Incubator--which will utilize the Integrated Security Operations Center and City data to improve student skills, research opportunities, and capabilities of cybersecurity product developers to create tools for defense. The Innovation Incubator seeks to introduce a unique "Cyber Range." The Cyber Range will establish a physical and online space--connected to the LA Cyber Lab information sharing platform and the City of Los Angeles's Integrated Security Operation Center (ISOC) to allow researchers, independent startups, and product developers the opportunities to enhance their security tools. The simulator will host an isolated virtual network for universities and companies to perform penetration testing, incident handling, ethical hacking, and forensic investigations to develop and improve their security products.

In addition, the LA Cyber Lab, as the next IS-ISAO, will host an annual cybersecurity summit as well as regular engagements including training seminars, monthly online meetings (for situational awareness and threat updates), and specialized conferences covering unique issues

(e.g. IoT security, Cloud Security, etc). ***Investments in tier three of this proposal will allow the LA Cyber Lab to engage a wider audience of constituents, from small and midsize companies to large corporations, and will offer a higher number of educational and career opportunities for all citizens.***

Ultimately, this funding will allow the Cyber Lab to become a cost-effective, transparent IS-ISAO that can easily be replicated in other risk areas of the United States. Leveraging the Cyber Lab's cutting edge infrastructure and existing information-sharing arrangements, this cooperative agreement will amplify the online resilience of State, Local, Territorial and Tribal (SLTT) governments by enhancing their capabilities to prepare for, defend against, respond to, and recover from cyberattacks.

II. Background

The nature of the cybersecurity threat in the United States mandates the need for leadership in preventing, mitigating, and recovering from adverse events in cyberspace. As the recent attacks on the U.S. Office of Personnel Management, the Democratic National Committee, Sony Pictures Entertainment, and the City of Atlanta indicate, there is a critical need for enhanced bilateral information-sharing, cybersecurity workforce and education development, multifaceted incident response strategies, and protection of critical infrastructure. Failing to invest in a culture of cybersecurity collaboration and information-sharing, particularly among SLTT governments and the private sector, could have potentially devastating consequences for the national and economic security of the nation.

City of Los Angeles

As America's second largest city, Los Angeles is both a center of gravity for economic prosperity and a sitting target for criminals, terrorists, and state-sponsored actors. While the city serves a critical economic conductor in the region, State of California, and the U.S. at large, it must also be resilient to physical and cyber threats that confront its critical infrastructure and key resources. Recognizing this, Eric Garcetti, Mayor of the City of Los Angeles, issued Executive Directive No. 2 (hereafter referred to as "ED2") on October 30th, 2013. Executive Directive No. 2 elevated cybersecurity as a public safety function of the city. It mandated cooperation among all city departments, between every department and the City's Information Technology Agency (ITA), and between the city and higher levels of government. ED2 established an intergovernmental body known as the Cyber Intrusion Command Center (CICC) which oversaw the development of the city's award-winning Integrated Security Operations Center (ISOC). The CICC--which brings together the cybersecurity managers of all city departments, including

proprietary departments, and incorporates assistance from the FBI, U.S. Secret Service, and U.S. Department of Homeland Security--has provided leadership through the following charges:

- Facilitating the identification and investigation of cyber threats and intrusions against city assets;
- Ensuring incidents are quickly, properly, and thoroughly investigated by the appropriate law enforcement agency;
- Facilitating dissemination of cybersecurity alerts and information;
- Providing uniform governance structure accountable to city leadership;
- Coordinating incident response and remediation across the city;
- Serving as an advisory body to city departments;
- Sponsoring independent security assessments to reduce security risks; and
- Ensuring awareness of best practices.

The City of Los Angeles' cybersecurity program has been brought to the attention of other U.S. municipalities and states seeking to streamline their own policy frameworks. At the recent 2018 Conference of Mayors in Boston, the U.S. Department of Homeland Security Undersecretary for the National Protection and Programs Directorate called Los Angeles the 'gold standard for cybersecurity resilience and defense.' Again at the 2018 National Conference of State Legislatures Cybersecurity Task Force, the SLTT Section Chief of DHS' NCCIC commended Los Angeles and asked that state participants refer to ED2 as a starting point for their own cybersecurity strategies. However, for all of the city's successes and accolades, Mayor Garcetti realized that government is not the only sector vulnerable to cyber threats nor can government be solely capable of confronting this complex challenge.

The Los Angeles Cyber Lab: A Public-Private Partnership for Cybersecurity

The private sector continues to be the target of malicious cyber intrusions. In recent years, Los Angeles has been victim to several high-level cyber attacks against the private sector. At the organizational level, these include sophisticated attacks such as data breaches on Sony Pictures Entertainment and Snap, Inc., and ransomware attacks on Hollywood Presbyterian Medical Center and AP Moller-Maersk (which affected the company's operations at the Port of Los Angeles). On the individual level, more than 3,500 cyber crimes were reported in Los Angeles last year alone, and city residents lost more than $14.3 million to attacks online.

Realizing this, in August 2017 the mayor announced the formation of the Los Angeles Cyber Lab--a first of its kind public-private partnership for cybersecurity. It is a non-profit organization dedicated to protecting the personal and proprietary information of Los Angeles

businesses and residents. The organization achieves this mission by facilitating and promoting innovation, education, and cybersecurity information-sharing between the public and private sectors. On the one hand, the City of Los Angeles has the capability to conduct multi-source analysis of cyber threat indicators and to collect critical intelligence on emerging threats. Naturally, the city is better positioned to investigate and prosecute cyber criminals and can leverage the support of federal resources and partners for threat identification and remediation. On the other hand, the private sector complements the city through its wide ownership of critical infrastructure exposed to attacks, its vast technological and financial capital, and its substantial cybersecurity expertise. The public-private partnership approach optimizes the Cyber Lab's ability to collect and disseminate cyber threats, to engage the public through education and training, and to expansively share cybersecurity best practices.

The Los Angeles Cyber Lab is dedicated to sharing the latest cybersecurity threat intelligence and alerts gathered by the City of Los Angeles and its public and private partners. A board of advisors, led by Mayor Eric Garcetti and consisting of the leadership of over 30 cross-sector businesses and government entities, develops policies and practices to help guide the Cyber Lab's mission. Membership in the Los Angeles Cyber Lab is open to all business and residents at zero cost. *Table 1* shows the breakdown of the Cyber Lab's advisory board members by sector:

Table 1. **Los Angeles Cyber Lab Partners (by Sector)**	
Energy and Utilities	Los Angeles Department of Water and Power
	Southern California Edison
Consulting	KPMG
	PWC
	West Monroe Partners
Health Care	Cedars-Sinai Medical Center
Financial	City National Bank
Transportation and Shipping	Los Angeles World Airports
	Port of Los Angeles
Information Technology	ByteCubed
	CGI

	Cisco Systems
	CSO Advisors
	Dell Technologies
	IBM
	Inverselogic
	Microsoft
Entertainment	21st Century Fox
	AEG
	Creative Artists Agency
	Hulu
	Oak View Group
	Riot Games
Telecommunication Services	Motorola Solutions
Government	California Office of Emergency Services
	City of Los Angeles
	Federal Bureau of Investigation
	Multi-State Information Sharing and Analysis Center (MS-ISAC)
	U.S. Department of Homeland Security
	U.S. Secret Service
Legal	O'Melveny and Myers
Consumer	Dollar Shave Club
	Westfield
Education	USC Information Sciences Institute
Non-Profit	Homeland Security Advisory Council
	National Cyber-Forensics and Training Alliance
	Secure The Village

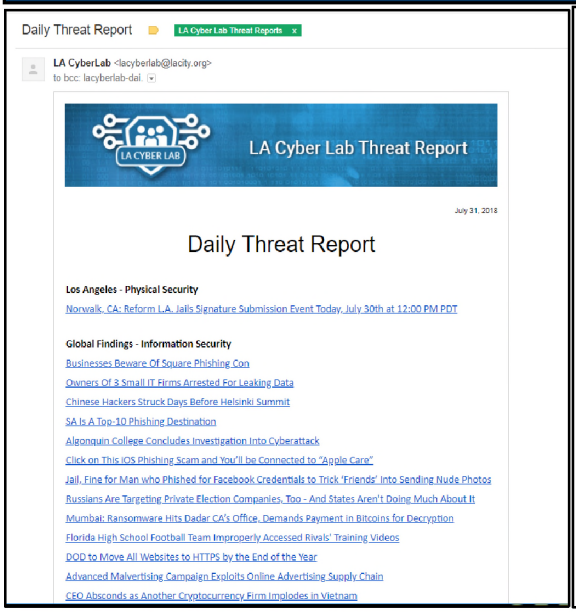
Los Angeles Cyber Lab Initiatives

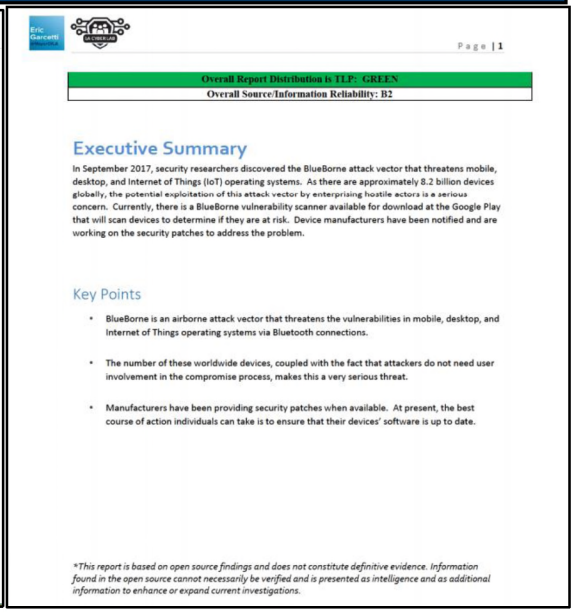
In order to achieve the Los Angeles Cyber Lab's mission, the organization's activities are focused around several major goals or initiatives. In cooperation with the advisory board and the Cyber Lab's state and federal partners, the organization sets the standards, policies, and metric objectives to gauge success in each initiatives. Three of the Cyber Lab's foundational initiatives are listed:

Los Angeles Cyber Lab Initiative I: Protection and Alerts

During initiative one, the Los Angeles Cyber Lab began sharing information generated from the City of Los Angeles' award-winning Integrated Security Operations Center (ISOC). The ISOC analyzes upwards of one billion security related events per day and also aggregates data from the federal government and key private sector sources. The Cyber Lab allows member organizations of all scopes and sizes to ingest critical cybersecurity data, alerts, Indicators of Compromise (IOCs), and threat reports generated every single day. This data is produced in user-friendly formats. See *Image 1* below for an example of threat intelligence products delivered to customers:

Image 1. **LA Cyber Lab Daily Threat Intelligence Products**





Los Angeles Cyber Lab Initiative II: Mutual Information Exchange

The Los Angeles Cyber Lab made history when it became one of the first entities in the nation to implement real-time information exchange with a private sector partner in April 2018.

The City of Los Angeles ISOC can publish to and receive from a variety of new sources, enabled by the STIX/TAXII standard format for sharing Indicators of Compromise (IOCs). Los Angeles Cyber Lab members can receive and contribute to the active defense of networks across Los Angeles and surrounding communities. Member organizations receive real-time, highly correlated/vetted feed of threat intelligence which directly assists information security teams in enhancing their security protections such as downloading relevant patches. One private sector partner has provided anecdotal feedback that--resulting from the company's participation in the mutual information sharing program--the company is blocking an average of 20% new and previously unseen threats. Cybersecurity experts have also shared with the Cyber Lab that a threshold of 15-20 large cross-sector organizations sharing their IOCs with ISOC will allow the organization to assess up to 90% of worldwide cyber threats.

Los Angeles Cyber Lab Initiative III: Innovation Incubator

The Los Angeles Cyber Lab's "Innovation Incubator" embodies three critical and interrelated objectives. First, the Cyber Lab hosts networking events for the business community for the purpose of connecting attendees to federal law enforcement resources and to cutting-edge practitioners in the cybersecurity field. Second, the lab partners with academia to provide cybersecurity career training for students with IT backgrounds as well as best practices for business executives. Third, slated for completion in 2019, the lab aspires to introduce a unique cyber "range" or simulator. The simulator aims to set aside physical and online space--connected to the city's ISOC and information-sharing platform--to allow researchers, independent startups, and product developers the opportunity to enhance their security tools. The simulator will host an isolated virtual network for universities and companies to perform penetration testing, incident handling, ethical hacking, and forensic investigations to develop and improve their security products.

III. Capacity to provide leadership in identification and development of a fully functional IS-ISAO (40 points)

a. The ability to conduct research and analysis on the most effective methods for bilateral cybersecurity information sharing in the SLTT community. (10 points).

In terms of quantitative threat intelligence, the Los Angeles Cyber Lab has taken comprehensive steps to identify the most effective methods for bilateral information-sharing. The LA Cyber Lab began with a landmark effort to share the latest cybersecurity intelligence gathered

by the City of Los Angeles, through its 41 municipal departments, including its port, airport, and utility departments, to businesses throughout the LA region. At its inception, the LA Cyber Lab was only capable of providing threat intelligence generated by the City of Los Angeles through PDF and CSV formats. While this was a useful start, the process of individually downloading files and manually updating IP/domain information was labor-intensive and heavily time-consuming. Thus, a target could be hit with malware in the timeframe before a network administrator could update their systems with new information. However, with investments in threat intelligence and analysis software, such as *SoltraEdge*, and security information and event management (SIEM) programs like *Splunk*, the Cyber Lab has been able to connect directly to the software solutions of other public and private sector partners. The STIX/TAXII standard format for sharing IOCs allows for rapid, real-time intelligence sharing with popular clients including *ThreatConnect* and *Anomali*. The Cyber Lab is also actively working with the DHS NCCIC's systems programmers to develop solutions that will allow private sector companies and public sector governments--those lacking sophisticated IT and security teams--to share their threat indicators as well. All threat indicators are directly sent to DHS NCCIC through the department's Automated Information Sharing (AIS) platform.

Moreover, while the City of Los Angeles already receives threat intelligence from other SLTT entities, including the State of California Governor's Office of Emergency Services (CalOES) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), it is currently in early talks with other SLTT jurisdictions including the Cities of Santa Monica, Beverly Hills, Culver City, the Counties of Los Angeles and San Bernardino, and the City of New York. Consequently, the LA Cyber Lab has the potential to become both a Southern California regional IS-ISAO and a transnational information-sharing entity.

In terms of qualitative threat intelligence, the Cyber Lab continues to send out user-friendly analytical reports to upwards of 500 small and midsize customers. The Cyber Lab's research has also found that having a centralized email address or similar communication portal allows customers to bi-laterally share qualitative information about phishing attempts, social media scams, disinformation campaigns, and other social engineering techniques. A future investment in the Cyber Lab will support ISOC programmers in developing an integrated, user-friendly portal to submit intelligence on cyber threats observed in the business sector.

b. Background with cybersecurity-related information sharing and the identification, development, and implementation of fully functional IS-ISAO that focus on regional information sharing, communications and outreach, training and education, research and

development for the improvement of State Local Tribal and Territorial (SLTT) government capabilities and capacity. (15 points).

Currently, the LA Cyber Lab primarily draws threat intelligence from the City of Los Angeles and multiple private sector partners. The City of Los Angeles' threat intelligence model is a decentralized one, in which analysts at four main hubs (the City's Information Technology Agency, the Port of Los Angeles, the Department of Water & Power, and Los Angeles World Airports) employ their own cyber threat analysts to detect and mitigate threats, but communicate through a central platform, the Integrated Security Operations Center (ISOC). The ISOC can be staffed, at any point in time, with up to eight full-time cyber threat analysts. It is overseen by a Chief Information Security Officer with over twenty years of expertise defending the information systems of Los Angeles' mission critical departments (including the Port of Los Angeles and the Information Technology Agency). The lab's cyber threat analysts are highly trained to identify threats, correlate and assign confidence values to threat indicators and are skilled in incident handling. The ISOC is co-located at the City of Los Angeles Emergency Operations Center so that in the event of an act of cyber-terrorism, the Mayor, the cyber threat analysts, Cyber Lab's federal law enforcement partners, and private sector experts can join together and coordinate disaster recovery efforts.

By drawing upon the ISOC and the LA Cyber Lab's business members, the Los Angeles Cyber Lab has the infrastructure necessary to develop into a fully functional IS-ISAO. The Cyber Lab is capable of bilateral information-sharing between the City of Los Angeles, other SLTT jurisdictions, private companies from across multiple sectors, and national customers. The Cyber Lab conducts widespread communication and outreach efforts, offers training and continued education opportunities for students and practitioners (in conjunction with the lab's private sector InfoSec experts), and is actively seeking ways to integrate the capabilities of other SLTT jurisdictions.

c. Qualified and experienced to gather, analyze, and disseminate government and critical infrastructure information to SLTT. Recent and extensive experience providing cybersecurity-related information sharing and best practice development generally. (15 points).

The Los Angeles Cyber Lab, through the Integrated Security Operations Center, conducts a Critical Asset Protection (CAP) program. The CAP Program inventories top public online critical assets so that the ISOC can focus resources for elevated monitoring and risk assessment

specifically on assets that are vital to the safety and core operations of the City. CAP clearly defines which network-connected assets are most important based on revenue, reputation, and core operational impact. Through the ISOC's intelligence analysis and information-platform, it has the ability to disseminate critical infrastructure information to SLTT governments just as it currently does with the Department of Homeland Security. Expanding this approach to the LA Cyber Lab's private sector partners and SLTT governments makes it possible to target special resources to the most critical areas of operation in the region.

IV. Develop documentation including design, policies and procedures, CONOPS, and operations manual(s)

a. Develops policy and procedures to provide escalation to law enforcement, Department of Homeland Security, and to national security within SLTT community, regional activity and awareness across the network. (10 points).

The Los Angeles Cyber Lab operates in coordination with the City of Los Angeles Cyber Intrusion Command Center (CICC). The CICC adopted a Cyber Incident Response Policy (CIRP) effective May 18, 2016. The policy outlines the procedures for city departments for responding to cybersecurity incidents and maintaining continuity of operations, especially in critical infrastructure sectors (harbor, airports). It specifically initiates protocols for the following stages of a cyberattack response:

- Confirming whether an incident occurred;
- Providing a defined incident notification process;
- Promoting the accumulation and documentation of accurate information;
- Establishing controls for proper retrieval and handling of evidence;
- Containing the incident and stopping any unwanted activity quickly and efficiently;
- Minimizing disruption to computing operations;
- Providing accurate reports and useful recommendations to management; and
- Preventing and/or mitigating future incidents from occurring.

Furthermore, the policy outlines the procedures for incident escalation and communication with law enforcement and national security partners within the SLTT community. Should a cybersecurity incident require higher assistance, the following external entities have direct channels for support: Multi-State Information Sharing and Analysis Center (MS-ISAC); Federal Bureau of Investigation (FBI); United States Secret Service (USSS); Electronic Crimes

Task Force (ECTF); Department of Homeland Security, National Cybersecurity and Communications Integration Center (DHS NCCIC); Joint Regional Intelligence Center (JRIC). This escalation procedure can easily be adopted by other SLTT jurisdictions, ISACs, ISAOs, and private sector companies.

V. Capacity to Provide Wide Outreach

a. Ability to deliver transparent coordination engagements with existing ISACs, ISAOs, associations, SLTT, private companies, Federal agencies, and subject matter experts engaged in cybersecurity-related information sharing supporting their customers. (10 points)

The Los Angeles Cyber Lab currently operates direct, bilateral channels with the Multi-State Information Sharing and Analysis Center (MS-ISAC). Staff plans to adopt this model and apply it to other ISAC relationships including with the Election Infrastructure ISAC, and the Information Technology ISAC. LA Cyber Lab is coordinating engagements with other nationwide and global cybersecurity associations including the Global Cyber Alliance (GCA), 100 Resilient Cities (100RC), the National Cyber Security Alliance (NCSA), the Cyber Threat Alliance (CTA), and the IoT Cybersecurity Alliance. These engagements will allow the IS-ISAO to be integrated in a community of industry-leading cyber experts which will benefit the lab's private sector members, and ultimately SLTT governments. One possibility is for the LA Cyber Lab--as the IS-ISAO--to lead a national council of the ISACs, ISAOs, and associations in the cybersecurity community. The U.S. Department of Homeland Security would play an important programmatic and policy role in the development of the council. This would permit for smoother information-sharing between the council, SLTT governments, and DHS.

b. Ability to work with academic partners who will utilize IS-ISAO operations centers to provide real world learning environments to improve student skills and identify research opportunities for students and faculty to explore the full spectrum of cyber technology. (10 points).

One of the core pillars of the Los Angeles Cyber Lab is academic training and cybersecurity research and development. Through the city's Data Science Federation, the Cyber Lab has formal arrangements with the University of California, California State University, University of Southern California, Los Angeles Community College, California Polytechnic Pomona, Claremont Graduate School, California Institute of Technology, Pepperdine University, Loyola Marymount University, and Occidental College. Students and professors can work with

the LA Cyber Lab in a variety of ways, including paid internships, challenges worked inside a classroom setting, interactive partnerships between the class and lab, volunteerships, and internships for course credit.

The Cyber Lab brings in--and will continue to bring--teams of researchers (professors, graduate students, undergraduate students) to improve student skills and develop cutting-edge solutions to latest cybersecurity challenges. For example, in late September 2018, the Los Angeles Cyber Lab will bring in a team of academics from California State University Dominguez Hills to develop tools for the Integrated Security Operations Center (ISOC). The ISOC registers upwards of one billion events per day from systems throughout the city to analyze and detect security-related incidents and threats. The goal of the CSU researchers' project is to use the data collected by the ISOC to provide situational awareness and predictive analysis of past, current and future cyber threats. The students will provide deliverables such as dashboards and visualizations of cyber risks. As a potential IS-ISAO, the LA Cyber Lab can provide these tools (free-of-charge) to customers including private sector companies, SLTT governments, and federal partners.

c. Ability to develop hands-on workforce development programs in collaboration with academia. (10 Points).

The Los Angeles Cyber Lab hosts free career training and networking events for local universities and other relevant associations. As a component of initiative three, the objective is to create an academia-to-workforce pipeline targeting students in tech and cyber. With an estimated 300,000 open positions in cybersecurity in the United States and over 10,000 of those jobs in the Los Angeles/Long Beach metro area, there is a critical need to introduce more people to the well-paying careers available.

One notable area of cooperation worth mentioning is the Cyber Lab's relationship with the U.S. Department of Commerce's National Initiative for Cyber Security Education (NICE) and the U.S. Department of Labor's Task Force on Apprenticeship Expansion. The lab plans to coordinate engagements--in conjunction with our academic partners in the Data Science Federation--where private sector companies from the Cyber Lab advisory board and beyond can exchange information and network with college and university career staff. This will enable the critical flow of students to highly demanded cybersecurity career positions. With funding to the IS-ISAO, the Cyber Lab can expand development programs to include career switchers, those re-entering the workforce, transitioning military, and more.

d. Ability to coordinate and engage with owners and operators and regulators of critical infrastructure, relevant agencies, and other public and private sector stakeholders. (10 points).

As stated in this narrative's background, the Los Angeles Cyber Lab has formal relationships with the owners and operators of critical infrastructure from across many fundamental sectors including finance, energy & utilities, telecommunications, healthcare, and information technology. The Cyber Lab currently shares threat intelligence information with both public and private owners of critical infrastructure and, importantly, the lab bilaterally receives unique information from its customers. For example, a malicious IP connection seen on the networks of Los Angeles World Airports is pushed to the Cyber Lab, vetted, and then identified as an Indicator of Compromise (IOC). Once labeled an IOC, it is published in real time to the Cyber Lab's customers including other owners of critical infrastructure. As a result, the situational awareness provided via the Cyber Lab's mutual information sharing program benefits all public and private entities in all critical sectors, thereby ensuring economic and physical security across the region and nation.

VI. Cost-Effectiveness and Budget Narrative

a. The extent to which the applicant's proposed budget shows an effective use of grant funds. (10 points)

Tier 1 Funds--IS-ISAO Information Sharing Platform and Technology Acquisitions

Component	Description/Justification	Costs
Threat Intelligence, Analysis, and Sharing Platform (TIASP)	• Estimated cost of hardware, software, and application development services required to build a universal cyber threat intelligence collection, analysis and distribution system = $1,600,000 • Estimated contracted support services for integration with trusted threat intelligence partners (ISOC, MS-ISAC, DHS-NCCIC AIS, FBI and private security vendors), private sector partners, and SLTT governments = $210,000	$1,810,000
Total		**$1,810,000**

Tier 2 Funds--Building Out IS-ISAO Personnel and Infrastructure *

Component	Description/Justification	Costs
Executive Director (ED) / Chief Development Officer (CDO)	The ED/CDO will establish internal infrastructure to ensure long-term sustainability of the IS-ISAO through sponsorship activities, outreach, to cover costs of outreach, personnel, information-sharing system maintenance, and other Cyber Lab expenses following the grant's completion. ● Relative cost of a contractor based on U.S. OPM GS-0340 Series = GS12, Step 5 = $94,115	$94,115
Policy Director	The Policy Director will develop documentation including design, policies and procedures, CONOPS, and operations manuals. Responsible for researching information-sharing best practices and advising/consulting with private sector, SLTT, and federal partners. ● Relative cost of a contractor based on U.S. OPM GS-2210 Series = GS9, Step 5 = $64,900	$64,900
Program Director	The Program Director will coordinate the Cyber Lab's annual summit, as well as the regular conferences, cybersecurity training courses, and other outreach events. ● Relative cost of a contractor based on U.S. OPM GS-0340 Series = GS9, Step 5 = $64,900	$64,900
Cyber Threat Analyst (x2)	Two cyber threat analysts will supplement existing analysts at the Integrated Security Operations Center. Whereas the current analysts are mostly focused on situational awareness and incident handling, the two new threat analysts will be fully dedicated to supporting information-sharing with private sector entities, SLTT governments, and national customers. ● Relative cost of a contractor based on U.S. OPM GS-0132 Series = GS13, Step 5 = $111,914 x 2 = $223,828	$223,828
Total		**$447,743**

** Estimated contractor salaries are based on the U.S. Office of Personnel Management's (OPM) General Schedule (GS) scale incorporating the 1.4% general schedule increase and a locality payment of 30.57% for the locality pay area of Los Angeles-Long Beach, CA.*

Tier 3 Funds--Institutionalizing IS-ISAO Innovation Incubator (Range) and Stakeholder Outreach/Engagement Program

Component	Description/Justification	Costs
Innovation Incubator (Range) / Academic Learning Environment	• Estimated cost of designing the facility including the lab consoles, the display wall, audio/visual, and computer equipment (starting with 30 users) = $150,000 • Estimated cost of contracting an organization which which can develop cyber range services including simulated traffic and replicated network services such as webpages, browsers, and email = $120,000	$270,000
Stakeholder Engagement: LA Cyber Lab Summit; Regular Meetings, and Conferences	• Estimated cost for contractor to develop a one-time LA Cyber Lab Summit with the inclusive costs of venue, materials, support & implementation services to organize the event, and to develop a white-paper summary that will serve as an After Action Report (AAR) = $100,000 • Estimated cost of a single monthly online or teleconference call with IS-ISAO members (video conferencing service for enterprise) = $20 x 12 months = $120 • Estimated cost of a single quarterly conference or event presentation with SLTT governments, the private sector, and national partners (to include venue, materials, support & implementation services to organize the event, and to develop an After Action Report (AAR) = $15,000 x 4 quarters = $60,000 • Estimated cost of a single bi-annual cybersecurity training event (to include venue, materials, support & implementation services to organize the event) = $10,000 x 2 events = $20,000	$180,120
Marketing and Management Materials	• Estimated support/maintenance costs and marketing materials including those needed to develop PSAs, banners and educational items for outreach, as well as additional staff supplies = $135,000	$135,000
Total		**$585,120**

Grant Management and Administration (M&A) Sub-recipient Agreement

Component	Description/Justification	Costs
Grant Management and Administration (M&A)	• The Los Angeles Mayor's Office of Public Safety (Grants & Management Division) will manage all fiscal obligations, ensuring that invoicing, documentation of expenditures, and payments are conducted timely and in accordance with DHS guidelines, award conditions, and federal regulations. The Mayor's Office will also manage the procurement of contractual services outlined in the grant award in compliance with these requirements and federal procurement rules. • The LA Cyber Lab will retain complete oversight, management, and programmatic control of the project, make any equipment, hardware/software purchases, and manage performance to ensure that all deliverables are completed within the performance period. The LA Cyber Lab will maintain responsibility for providing all regular reporting, performance metrics, and budgets to DHS. • Procedurally, this will be accomplished by the LA Cyber Lab executing a sub-recipient agreement with the Mayor's Office under which the Mayor's Office, as the sub-recipient, will agree to conduct M&A functions for the LA Cyber Lab, as the grantee. The Mayor's Office will create two separate accounts—one for M&A fees and one for contractual services. As contractual services work is performed, LA Cyber Lab's authorized representatives will approve the work, and transfer funds to the City, which in turn, will issue payments to contractors upon presentation of satisfactory documentation. This ensures that the LA Cyber Lab maintains authority over the project deliverables while the City holds responsibility for compliance with fiscal requirements. • Five percent (5%) of the grant award will be dedicated for fiscal administration of grant-funded projects to ensure compliance with objectives, timeline and grantor requirements. • $3,000,000 x 5% = $150,000	$150,000
Total		**$150,000**

Grand Total		**$2,992,863**

Attachment 4

RESOLUTIONS OF THE MEETING OF THE BOARD OF DIRECTORS

OF

LOS ANGELES CYBER LAB, INC.
A California Nonprofit Public Benefit Corporation

on

December 7, 2018

The members of the Board of Directors (the "**Board**") of Los Angeles Cyber Lab Inc., a California nonprofit public benefit corporation (the "**Corporation**"), hereby adopt the following recitals and resolutions, effective as of December 7, 2018.

WHEREAS, the Corporation applied for and was awarded the "Los Angeles Cyber Lab: A Internet Security – Information Sharing and Analysis Organization (IS-ISAO) Pilot" Grant provided by the U.S. Department of Homeland Security ("**DHS**" or "**Grantor**") through Funding Opportunity Number DHS-18-NPPD-128-ISAO-001 (the "**ISAO Grant**"), in the amount of $2,992,863, with a grant performance period of September 30, 2018 through September 29, 2019.

RESOLVED, that the Corporation is hereby authorized accept the ISAO Grant from DHS, in the amount of $2,992,863, with a grant performance period of October 1, 2018 through September 30, 2019.

RESOLVED, that the Corporation is hereby authorized to execute for and on behalf of the Corporation, any actions necessary for the purpose of obtaining federal financial assistance under the ISAO Grant.

RESOLVED, that the Corporation is hereby authorized to make expenditures of the ISAO Grant funds in accordance with the approved grant budget and written authorization of the Grantor.

WHEREAS, the Board considered a proposal, wherein the City of Los Angeles Mayor's Office would be designated by DHS as the administrator and fiscal agent of the ISAO Grant on behalf of the Corporation. DHS has approved the use of approximately 5% of the total award - $150,0000 – to be used in support of the management and administration (M&A) of this grant. The Mayor's Office would allocate these funds towards salary and fringe benefits of the Mayor's Office grant, contract, and fiscal management teams. Duties would include grant monitoring and reporting, grant guideline compliance, coordination and communication with DHS and general program management. Fiscal specialists in the Mayor's Office shall ensure the timely, accurate, and appropriate approval of all grant expenditures, as well as maintaining all necessary documentation to ensure compliance with federal grant accounting regulations.

WHEREAS, that the Directors not employed by or otherwise affiliated with the City considered, without the City-employed or affiliated directors present, whether this delegation of authority to the Mayor's Office creates a conflict of interest under the Corporation's Conflict of Interest Policy and determined that a conflict of interest does not exist, provided that no Director of the Corporation shall receive any compensation or other interest in connection with the delegation of responsibility or the sub-award of grant funds to the City.

RESOLVED, that the Corporation agrees to the designation of the City of Los Angeles Mayor's Office as the administrator and fiscal agent for this grant on behalf of the Corporation, and shall allocate $150,000 of grant funds to the City for this purpose.

WHEREAS, the Corporation considered a proposal to use a portion of the grant funds towards hiring a cybersecurity threat analyst and a security data scientist for the LA Cyber Lab, such consultants to be selected and hired by the City of Los Angeles Information Technology ("ITA") through an IT professional services agency under contract with the City.

RESOLVED, that the Corporation approves of the expenditure of grant funds by the City to hire a cybersecurity threat analyst and security data scientist for a term of nine months during the performance period of the grant (January 1, 2019 to September 29, 2019), for a combined amount not to exceed $280,000.

RESOLVED, that the Corporation is hereby authorized to negotiate and execute an agreement with the City of Los Angeles an amount not to exceed $430,000 to the City of Los Angeles, in accordance with the approved grant budget, for the purpose of: (1) managing and administering the ISAO Grant on behalf of the Corporation, in an amount not to exceed $150,000, as detailed in the above recitals and resolutions; and (2) contracting with an IT professional services agency to provide a full time cybersecurity threat analyst and security data scientist who will support threat information sharing between the City, the LA Cyber Lab, private sector entities, and other state and local jurisdictions, for a term of nine months during the grant performance period, for an amount not to exceed $280,000, as detailed in the above recitals and resolutions.

WHEREAS, the Corporation considered a proposal to use a portion of the grant funds towards hiring a consultant to serve as the Executive Director/Chief Development Officer of the LA Cyber Lab for the term of eight months during the performance period of the grant (February 1, 2019 to September 29, 2019). The Board considered Joshua Belk, of OpSec360 as

a candidate for this position, at a cost of $100,000. This expenditure is subject to the pending approval of the Grantor.

RESOLVED, that, subject to approval of the Grantor, the Corporation is hereby authorized to negotiate and execute a consulting agreement with OpSec360 for the services of Mr. Belk as Executive Director/Chief Development Officer of the Corporation, for a term of eight months during the performance period of the grant, for $100,000.

RESOLVED, that the officers of the Corporation be, and each of them hereby is, authorized and empowered, in the name and on behalf of the Corporation, to take such further actions and to execute such further documents relating to or contemplated by any of the foregoing resolutions, the taking of such actions or the execution and delivery of such documents to be conclusive evidence thereof.

RESOLVED, that any document heretofore executed and any action heretofore taken by any officer of the Corporation in furtherance of the business of the Corporation otherwise permitted under or contemplated by these resolutions be, and each of them hereby is, ratified, confirmed and approved for all purposes and in all respects.

Passed and approved this _____ day of _____, 2018.