The Department of Homeland Security (DHS)
Notice of Funding Opportunity (NOFO)
State, Local, Tribal and Territorial
Security Operations Center | Information Sharing and Analysis Center

All entities wishing to do business with the federal government must have a unique entity identifier (UEI). The UEI number is issued by the SAM system. Sam.gov information can be found at: https://sam.gov/content/entity-registration.

Grants.gov registration information can be found at:
https://www.grants.gov/web/grants/register.html.

Planned UEI Updates in Grant Application Forms

On April 4, 2022, the Data Universal Numbering System (DUNS) Number was replaced by a new, non-proprietary identifier requested in, and assigned by, the System for Award Management (SAM.gov). This new identifier is the Unique Entity Identifier (UEI).

Additional Information can be found on Grants.gov:

https://www.grants.gov/web/grants/forms/planned-uei-updates.html

A. Program Description

1. **Issued By**
   U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), Cybersecurity Division (CSD)

2. **Assistance Listings Number**
   97.123

3. **Assistance Listings Title**
   State, Local, Tribal and Territorial (SLTT) Security Operations Center (SOC) | Information Sharing and Analysis Center (ISAC)

4. **Funding Opportunity Title**
   State, Local, Tribal and Territorial (SLTT) Security Operations Center (SOC) | Information Sharing and Analysis Center (ISAC)

5. **Funding Opportunity Number**
   DHS-23-CISA-123-ISAC000001

6. Authorizing Authority for Program
Homeland Security Act of 2002, Pub. L. No. 107-296, § 102(b)(2) (codified as amended at 6 U.S.C. § 112(b)(2))

7. Appropriation Authority for Program

Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, Division F – Department of Homeland Security Appropriations Act, 2023, Title III – Protection, Preparedness, Response, and Recovery, Cybersecurity and Infrastructure Security Agency

8. Announcement Type
Initial (Year 1 of 2)

9. Program Overview, Objectives, and Priorities

Overview: Pulling together critical infrastructure communities is essential to the protection of critical infrastructure and to furthering cybersecurity for the nation. This program addresses the DHS mission to Secure Cyberspace and Critical Infrastructure, as defined in the U.S. Department of Homeland Security Strategic Plan – Fiscal Years 2020-2024, providing a funding methodology to support the state, local, tribal and territorial (SLTT) government, to include Elections, cyber ecosystem through capacity building and cyber threat information sharing among the nationwide trusted community of members. This program leverages the strength of market technology forces to spur innovative strategies within the Security and Operations Center (SOC) to enable a cyber-relevant Information Sharing and Analysis Center (ISAC) operating model that is consistent with section 2209 of the Homeland Security Act, Executive Order 13636, Executive Order 13691, and Presidential Decision Directive-63 (PDD-63). Specifically, section 2209(d)(1)(E) of the Homeland Security Act of 2002 requires the composition of the statutory national cybersecurity and communications center—a function now carried out by CISA's Cybersecurity Division—to include "an entity that collaborates with State and local governments on cybersecurity risks and incidents". This ISAC program convenes effective tools, managed services, analytic resources, and technology platforms for maintaining trust and collaboration across a coalition of SLTT and Elections members. It links the community to a nationwide cross domain threat information sharing capability, which enhances situational awareness and provides security readiness to face current threats in the digital battlefront. The short-term impact of services will allow SLTT and its subsector stakeholders to consume and exchange awareness of threats via technologies that serve to derive a more accurate and timelier picture of prioritized cyber defense actions.

Recognizing that DHS has complementary resources to support the ability of the SLTT sector (including critical sub-sectors such as Elections) to share cyber threat information, CISA is expanding its operational coordination with the ISAC in order to provide Federal level enrichment of cyber threats within the threat intelligence

platform, support risk prioritization, coordinate resilience efforts, and provide a communications infrastructure across national regions to include escalation and collaboration with appropriate law enforcement and intelligence agencies. The Recipient will work in partnership with and receive technical integration assistance from a CISA team. In addition, the Recipient must coordinate substantially with cyber threat experts from across the federal government. After the funding period has ended, the funding and supporting offices will continue to be available to provide technical assistance to ensure that information sharing, and collaboration continues.

The awardee will have access to sustained coordination with federal partners to defend forward and prevent or thwart malicious cyberspace actors and activities. Thus, through these efforts, the awardee will make improvements in the SLTT cyber ecosystem and the development of its workforce; provide for a more efficient response and recovery time of systems during attack; and develop resilience capabilities for our nation's SLTT government sector and critical subsectors (e.g., Elections).

Objectives: The purpose of this cooperative agreement is to expedite building an automated and streamlined capacity to share cyber threat information bi-directionally and collaboratively amongst the SLTT/Elections and CISA, as well as provide a mechanism for rapid adoption and methods to integrate with local activities in the SLTT environment that improve cyber security awareness and equip stakeholders to act in response to prioritized cyber threat information shared within the threat intelligence platform. Furthermore, this agreement will expand implementation of cyber managed services (e.g., National Prevention Pilot, End-Point Detection and Response Pilot, Malicious Domain Blocking and Reporting, Cyber Incident Response, Albert, Managed Email Security), for SLTT and the Elections subsector, and in so doing will impact the capabilities to create a more robust cyber defense and information sharing environment for the entire SLTT sector.

This Notice of Funding Opportunity Announcement (NOFO) is intended to fill a gap by providing supplemental resources to enable innovation, broaden centralized access to cyber threat information and communications platforms, provide for workforce development, and enhance cyber readiness and resilience, all while connecting the cyber ecosystems of the SLTT communities. By providing funds, technical assistance, and access to federal resources, it is expected that the Recipient will be able to:

a. Focus more of its business and resources on cyber threat information enrichment, scoring, and collaboration based on Indicators of Compromise (IOC)s derived from SLTT and its subsector infrastructure, ISAC information sources, open-source information, and external intelligence enrichment.
b. Create a lower entry cost for SLTT/subsector organizations (including elections infrastructure) who need help in managing cyber defenses and risk.
c. Expand the trusted SLTT/Elections subsector community) base that shares and collaborates on threat intelligence.

d. Provide some level of free managed security services and cyber threat information sharing services to the SLTT sector and its subsectors.

The government encourages developing the mechanism to collaborate on a single application if doing so would strengthen the overall capacity of the ISAC.

By technically integrating the SLTT cyber ecosystem and empowering cyber expertise and situational awareness across the SLTT trusted circle of members, the community will collaboratively serve to protect and improve defenses for the nation's SLTT and its critical infrastructure sub-sectors, foremost Elections.

Priorities: CISA will leverage this Cooperative Agreement award to advance SLTT cybersecurity risk management and to help build a healthy and resilient SLTT cyber ecosystem via automated collective community action. Successful execution of this agreement will focus on expanding SLTT sector interrelationships within the community using rapid rollout technology to enhance cyber threat information exchange.

The priority is to provide a connective platform among the SLTT cyber coordinators for collaborative threat intelligence sharing. This enhanced technical model relies upon trusted SLTT collaboration, elastic infrastructure, managed security services and robust analytic orchestration and informed risk information to give cyber coordinators decision advantage, improve situational awareness and provide enhanced cyber defense.

See Appendix A for a detailed approach of priorities and metrics.

See Appendix B for major program status.

10. Performance Measures

Performance metrics will be implemented based on the detailed approach as defined in Appendix A, Task 10. The performance metrics program must routinely measure, analyze, and report qualitative and quantitative measures and metrics on SLTT member partnerships, the impact of SLTT cyber security incidents, the degree and effectiveness of sensor coverage, endpoint coverage, and consolidation of SLTT traffic across a prevention stack, as well as the effectiveness of the Recipient's threat scoring and sharing methodology amongst the SLTT community.

The grants officer will oversee the execution of the cooperative agreement and the performance of cooperative agreement execution based on input from the CISA program office, discussion with the awardee, and Program Performance Reporting Requirements (found in section F).

B. Federal Award Information

1. **Available Funding for the NOFO:** $43,003,000

2. **Projected number of Awards:** 1

3. **Maximum Award Amount:** n/a

4. **Period of Performance:** 24 months

5. **Projected Period of Performance Start Date(s):** 09/30/2023

6. **Projected Period of Performance End Date(s):** 09/29/2025

   Budget Period(s) for the NOFO: 09/30/2023 to 09/29/2024

   a. The available funding for the NOFO described above is for an initial 12-month budget period from 09/30/2023 to 09/29/2024.
   b. Funding for a second non-competitive continuation award for a 12-month budget period of 9/30/2024 to 9/29/2025 is conditioned on the availability of funds, satisfactory progress by the Recipient, program authority, compliance with the terms and conditions of the federal award, and a CISA determination that continued funding is in the best interests of the Government.
   c. Extensions to the period of performance for this program are allowed. Recipients may request a no-cost extension to complete all project activities. The request must be submitted 60 days prior to the expiration of the performance period. Requests for extensions are subject to approval by DHS.

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

   a. To facilitate appropriate involvement, during the period of this cooperative agreement, CISA PO and the Recipient will be in contact monthly and more frequently as appropriate to ensure successful execution. Specific tasks and activities that may be shared between the Recipient and CISA PO include but are not limited to:
      i. Providing strategic/tactical guidance and feedback in furtherance of the goals and objectives of the award.
      ii. Providing access to key staff groups and other varied technical and programmatic resources, subject matter expertise, liaising with

stakeholders and selecting meetings/panel members for carrying out the program.

iii. Reviewing and approving deliverables.
iv. Reviewing and approving substantive provisions of proposed subawards or contracts.
v. Ending an activity if performance specifications are not met.
vi. Exchanging bi-directional cyber threat information and building TTP (Tactics, Techniques and Procedures) context in furtherance of the objectives to enable a collective defense model.
vii. Exchanging unattributed and attributed cyber threat landscape information.
viii. Holding equity calls with federal officials on SLTT victim notifications.

b. CISA PO will be responsible for substantial involvement to include, but are not limited to the following:

i. CISA PO will provide substantial programmatic involvement during the performance period. Oversight services at the highest level are to keep CISA leadership apprised of the program status and to identify and quickly mitigate any threats to on-time and on-budget completion.
ii. Substantial federal involvement includes administrative activities such as monitoring and reviewing project phases. CISA PO will not direct or recommend that the Recipient enter a contract with a particular entity.
iii. CISA will provide promotional support of the SLTT SOC|ISAC program and its services with the goal of increasing SLTT trusted community interest and fulfilling the vision of an interconnected cyber ecosystem.
iv. CISA PO will provide administrative assistance related to security clearances to complete the approved scope of work.
v. CISA will allocate sufficient office space and communications, IT systems, telephones, and administrative supplies at CISA for cyber liaison officers to sit "side-by-side" with federal colleagues to facilitate effective unity of effort in the situational awareness assessment of the SLTT community that is used to prepare the national cyber assessment.
vi. CISA will provide reception and integration of the LNO team into CISA by identifying a single CISA staff member who is assigned the responsibility to assimilate the LNOs and provide the access they need to perform their functions.
vii. CISA will provide Homeland Security Information Network (HSIN) platform resources for trusted sharing of Sensitive but Unclassified Information with the SLTT community.
viii. CISA will assist in the establishment of partnerships, collaboration, and cooperation with SLTT, or private entities that may be necessary for carrying out the program.

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

xxiii. CISA PO will provide promotional support of the SLTT SOC|ISAC program and its services with the goal of increasing SLTT trusted community interest and fulfilling the vision of an interconnected cyber ecosystem.

xxiv. CISA PO will provide, when appropriate, subject matter experts (SMEs) and other varied technical and programmatic resources to support each component of the program as defined in Appendix A.

xxv. CISA PO representatives will attend and participate in appropriate meetings initiated by the Recipient.

xxvi. CISA PO will assist in the establishment of partnerships, collaboration, and cooperation with Federal, State, local, tribal, or territorial governments, or private entities that may be necessary for carrying out the project.

xxvii. CISA PO and the Recipient will exchange bi-directional cyber threat indicators and information in furtherance of the objectives and priorities delineated in Appendix A in order to enable a collective defense model.

xxviii. For purposes of maintaining cyber situational awareness of issues that affect reliability and resilience of the SLTT, CISA PO and the Recipient will exchange unattributed and attributed cyber threat landscape information.

xxix. CISA PO will make available office space at CISA PO for analysts to sit "side-by-side" with federal colleagues to provide the situational awareness assessment for the SLTT and Elections community that is used to prepare the national cyber assessment.

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

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

xxxii. CISA will, as the program support deems necessary, facilitate coordination to address cybersecurity risks and incidents, in the form of email, site visits, teleconferences, workshops, webinars, technical exchanges, sharing cyber threat indicators and vulnerabilities, cyber analytic and awareness products, training opportunities, tabletop exercises, and technical assistance upon request.

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

Engagement Division (SED), Integrated Operations Division (IOD), Emergency Communications Division (ECD), and Infrastructure Security Division (ISD).

C. Eligibility Information

1. Eligible Applicants

- For-profit organizations other than small businesses
- Small businesses
- Nonprofits with 501(c)(3) IRS status, other than institutions of higher education
- Nonprofits without 501(c)(3) IRS status, other than institutions of higher education

2. **Applicant Eligibility Criteria** (see above)

a. Entity needs to be performing some of the functions of a Cyber Information Sharing and Analysis Center.
b. Entity must possess the capacity to mature and expand a functioning 24x7x365 SOC to enable an ISAC.
c. Entity must be able to grow and unite stakeholder trust communities.
d. Entity must be able to retain cybersecurity analytic staff, including those with TS/SCI clearance.
e. Entity must be able to provide scalable access to cybersecurity information, tools, and best practices.
f. Entity must be able to analyze huge amounts of information in real-time to identify trends and prioritize cyber information for actionable insights.
g. Entity must be able to sustain a communications model that allows critical cybersecurity information to quickly be disseminated across SLTT.
h. Entity must be capable of enabling reliable outcomes in managing cyber-relevant threat intelligence, with the benefit of improved customer resilience.

Entities that do not meet the eligibility criteria will be considered ineligible.

3. Other Eligibility Criteria/Restrictions

DHS will not consider applications that do not adhere to one or more of the following requirements:

a. **Deadlines.** DHS will not accept late applications. Without exception, applications must be received by Grants.gov on or before the deadline in this announcement or they will not be considered.
b. **Application relevance.** Applications that do not address the purpose of this announcement will not be considered.
c. **Compliance and completeness.** Applications must substantially comply with the application submission instructions and requirements in this announcement, or they will not be considered.
d. **Proof of non-profit status.** Non-profit applicants and any proposed subrecipient of a non-profit must provide documentation of non-profit and/or public status. This requirement does not apply to for-profit applicants or proposed subrecipients. Any of the following constitutes

acceptable proof of non-profit status:

i. A reference to the applicant organization's listing in the Internal Revenue Service's (IRS) most recent list of tax-exempt organizations described in section 501(c)(3) of the IRS Code.
ii. A copy of a currently valid IRS tax exemption certificate.
1. A statement from a State taxing body, State attorney general, or other appropriate State official certifying that the applicant organization has a non-profit status and that none of the net earnings accrue to any private shareholders or individuals.

e. A certified copy of the organization's certificate of incorporation or similar document that clearly establishes non-profit status.
f. Any of the items in the subparagraphs immediately above for a State or national parent organization and a statement signed by the parent organization that the applicant organization is a local non-profit affiliate.
g. A signed statement on official letterhead by an official authorized to apply for cooperative agreement funds on behalf of the public entity will suffice.
h. In addition, DHS will not consider **multiple applications** from a single organization serving as the lead. If more than one application is submitted by a single organization as the lead, the later in time will be considered, unless the later application clearly indicates a unique role for that organization, other than as lead for this activity.

4. Cost Share or Match

The SLTT SOC ISAC Program has a 30% non-federal cost-share requirement. The Recipient contribution may be cash (hard match) and/or in-kind (soft match). Eligible SLTT SOC ISAC Program applicants must commit to the non-federal cost-share requirement at the time of application in an amount not less than 30% of the total project cost reflected in the application budget. If the total project ends up costing more, the Recipient is responsible for any additional costs. If the total project ends up costing less, the Recipient may owe CISA an amount required to ensure that the federal cost-share does not exceed 70%. Recipient For example, if CISA approves a Recipient total project cost under a federal award of $100,000, then the:

- Federal cost-share is 70 percent of $100,000 = $70,000
- Recipient cost-share is 30 percent of $100,000 = $30,000

Unless otherwise authorized by law, the Recipient may not use other federal grant funding towards the required non-federal cost-share under the SLTT SOC ISAC Program award. The Recipient's contribution must be specifically identified in the application as part of the budget. The non-federal contribution, whether cash or in-kind, can only be used for authorized cooperative agreement purposes and has the same eligibility requirements as the federal assistance funds themselves. The basis for

requiring a non-federal cost-share is to increase the amount of cybersecurity resources available to the SLTT community, assure local interest and involvement through financial participation, and hold down federal costs.

D. Application and Submission Information

1. Key Dates and Times

a. Application Start Date: 06/14/2023

b. Application Submission Deadline: 08/01/2023 at 11:59:59 PM [ET]

c. Other Key Dates

Event	Suggested Deadline for Completion
Initial Registration at SAM.gov (includes UEI issuance)	Four weeks before actual submission deadline
Obtaining a valid EIN	Four weeks before actual submission deadline
Updating SAM registration	Four weeks before actual submission deadline
Starting application in Grants.gov	Two weeks before actual submission deadline

2. Agreeing to Terms and Conditions of the Award

By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

3. Address to Request Application Package

Application forms and instructions are available at Grants.gov. To access these materials, go to http://www.grants.gov.

For a hardcopy of the full NOFO, please write or fax a request to:

Shareef Prater
Grants Officer, Grants and Financial Assistance Division

Email: shareef.prater@hq.dhs.gov Phone: 202-770-4776

In addition, the following Telephone Device for the Deaf (TDD) and/or Federal Information Relay Service (FIRS) number available for this Notice is:
1-800-518-4726 (Grants.gov Help Desk)

Applications will be processed through the Grants.gov portal.

4. Unique Entity identifier and System for Award Management (SAM)

Each applicant, unless they have a valid exception under 2 C.F.R. § 25.110, must:

a. Be registered in SAM.gov before application submission.
b. Provide a valid unique entity identifier in its application.
c. Continue to always maintain an active SAM registration with current information during the Federal Award process.

5. Steps Required to Submit an Application, Unique Entity Identifier, and System for Award Management (SAM)

To apply for an award under this program, all applicants must:

a. Have an account with https://login.gov/;
b. Register for, update, or verify their SAM account and ensure the account is active and Employer ID Number (EIN) before submitting the application.
c. Create a Grants.gov account.
d. Add a profile to a Grants.gov account.
e. Establish an Authorized Organizational Representative (AOR) in Grants.gov.
f. Submit application in Grants.gov; and
g. Continue to maintain an active SAM registration with current information, including information on a Recipient's immediate and highest-level owner and subsidiaries, as well on all predecessors that have been awarded a federal contract, grant, or cooperative agreement within the last 3 years, if applicable, at all times during which it has an active federal award or an application or plan under consideration by a federal awarding agency.

Applicants are advised that DHS may not make a federal award until the applicant has complied with all applicable SAM requirements. Therefore, an applicant's SAM registration must be active not only at the time of application, but also during the application review period and when DHS is ready to make a federal award. Further, as noted above, an applicant's or Recipient's SAM registration must remain active for the duration of an active federal award. If an applicant's SAM registration is expired at the time of application, expires during application review, or expires any other time before award, DHS may determine that the applicant is not qualified to receive a federal award and use that determination as a basis for making a federal award to another applicant.

6. Electronic Delivery

DHS is participating in the Grants.gov initiative to provide the grant and cooperative agreement community with a single site to find and apply for grant funding and cooperative agreement opportunities. DHS encourages or requires applicants to submit their applications online through Grants.gov, depending on the funding opportunity. For this funding opportunity, the DHS Grants and Financial Assistance Division (GFAD) requires applicants to submit applications through Grants.gov.

7. How to Register to Apply through Grants.gov

a. *Instructions*: Registering in Grants.gov is a multi-step process. Read the instructions below about registering to apply for DHS funds. Applicants should read the registration instructions carefully and prepare the information requested before beginning the registration process. Reviewing and assembling the required information before beginning the registration process will alleviate last-minute searches for required information.

The registration process can take up to four weeks to complete. Therefore, registration should be done in sufficient time to ensure it does not impact your ability to meet required application submission deadlines.

Organizations must have a *Unique Entity Identifier (UEI)* Number with an active System for Award Management (SAM) registration, and Grants.gov account to apply for grants and cooperative agreements. If individual applicants are eligible to apply for this funding opportunity, then you may begin with step 3, Create a Grants.gov account, listed below.

Creating a Grants.gov account can be completed online in minutes, but SAM registration may take several weeks. Therefore, an organization's registration should be done in sufficient time to ensure it does not impact the entity's ability to meet required application submission deadlines. Complete organization instructions can be found on Grants.gov here: https://www.grants.gov/web/grants/applicants/organization-registration.html.

1) *Register with SAM*: All organizations applying online through Grants.gov must register with the System for Award Management (SAM). Failure to register with SAM will prevent your organization from applying through Grants.gov. SAM registration must be renewed annually. Organizations will be issued a UEI number with the completed SAM registration.

   For more detailed instructions for registering with SAM, refer to: https://www.grants.gov/web/grants/applicants/organization-registration/step-2-register-with-sam.html.

2) *Create a Grants.gov Account*: The next step is to register an account with Grants.gov. Follow the on-screen instructions or refer to the detailed instructions here: https://www.grants.gov/web/grants/applicants/registration.html.

3) *Add a Profile to a Grants.gov Account*: A profile in Grants.gov corresponds to a single applicant organization the user represents (i.e., an applicant) or an individual applicant. If you work for or consult with multiple organizations and have a profile for each, you may log in to one Grants.gov account to access all your grant and cooperative agreement applications. To add an organizational

profile to your Grants.gov account, enter the UEI Number for the organization in the UEI field while adding a profile.

- For more detailed instructions about creating a profile on Grants.gov, refer to: https://www.grants.gov/web/grants/applicants/registration/add-profile.html.

4) *EBiz POC Authorized Profile Roles*: After you register with Grants.gov and create an Organization Applicant Profile, the organization applicant's request for Grants.gov roles and access are sent to the EBiz POC. The EBiz POC will then log in to Grants.gov and authorize the appropriate roles, which may include the AOR role, thereby giving you permission to complete and submit applications on behalf of the organization. You will be able to submit your application online any time after you have been assigned the AOR role.

   For more detailed instructions about creating a profile on Grants.gov, refer to: https://www.grants.gov/web/grants/applicants/registration/authorize-roles.html.

5) *Track Role Status*: To track your role request, refer to: https://www.grants.gov/web/grants/applicants/registration/track-role-status.html.

6) *Electronic Signature*: When applications are submitted through Grants.gov, the name of the organization applicant with the AOR role that submitted the application is inserted into the signature line of the application, serving as the electronic signature. The EBiz POC **must** authorize people who are able to make legally binding commitments on behalf of the organization as a user with the AOR role; **this step is often missed, and it is crucial for valid and timely submissions.**

8. How to submit an Application to DHS via Grants.gov

Grants.gov applicants can apply online using Workspace. Workspace is a shared, online environment where members of a team may simultaneously access and edit different webforms within an application. For each NOFO, you can create individual instances of a workspace.

Below is an overview of applying on Grants.gov. For access to complete instructions on how to apply for opportunities using Workspace, refer to: https://www.grants.gov/web/grants/applicants/workspace-overview.html.

a. *Create a Workspace*: Creating a workspace allows you to complete it online and route it through your organization for review before submitting.

b. *Complete a Workspace*: Add participants to the workspace to work on the application together, complete all the required forms online or by downloading PDF versions, and check for errors before submission. The Workspace progress bar will display the state of your application process as you apply. As you apply using Workspace, you may

click the blue question mark icon near the upper-right corner of each page to access context-sensitive help.

c. *Adobe Reader*: If you decide not to apply by filling out webforms you can download individual PDF forms in Workspace. The individual PDF forms can be downloaded and saved to your local device storage, network drive(s), or external drives, then accessed through Adobe Reader.

   NOTE: Visit the Adobe Software Compatibility page on Grants.gov to download the appropriate version of the software at: https://www.grants.gov/web/grants/applicants/adobe-software-compatibility.html.

d. *Mandatory Fields in Forms*: In the forms, you will note fields marked with an asterisk and a different background color. These fields are mandatory fields that must be completed to successfully submit your application.

e. *Complete SF-424 Fields First*: The forms are designed to fill in common required fields across other forms, such as the applicant's name, address, and UEI number. To trigger this feature, an applicant must complete the SF-424 information first. Once it is completed, the information will transfer to the other forms.

f. *Submit a Workspace*: An application may be submitted through workspace by clicking the Sign and Submit button on the Manage Workspace page, under the Forms tab. Grants.gov recommends submitting your application package at least 24-48 hours prior to the close date to provide you with time to correct any potential technical issues that may disrupt the application submission.

g. *Track a Workspace Submission*: After successfully submitting a workspace application, a Grants.gov Tracking Number (GRANTXXXXXXXX) is automatically assigned to the application. The number will be listed on the Confirmation page that is generated after submission. Using the tracking number, access the Track My Application page under the Applicants tab or the Details tab in the submitted workspace.

   - For additional training resources, including video tutorials, refer to: https://www.grants.gov/web/grants/applicants/applicant-training.html.

   Applicant Support: Grants.gov provides applicants 24/7 support via the toll-free number 1-800-518-4726 and email at support@grants.gov. For questions related to the specific Cooperative Agreement opportunity, contact the number listed in the application package of the Cooperative Agreement to which you are applying.

   If you are experiencing difficulties with your submission, it is best to call the Grants.gov Support Center and get a ticket number. The Support Center ticket

number will assist DHS with tracking your issue and understanding background information on the issue.

9. Submitting the Final Application in *[another grant system]* N/A

10. Timely Receipt Requirements and Proof of Timely Submission

a. *Online Submission.* All applications must be received by **MIDNIGHT Eastern time** on the due date established for each program. Proof of timely submission is automatically recorded by Grants.gov. An electronic date/time stamp is generated within the system when the application is successfully received by Grants.gov. The applicant with the AOR role who submitted the application will receive an acknowledgement of receipt and a tracking number (XXXXXXXX) from Grants.gov with the successful transmission of their application. This applicant with the AOR role will also receive the official date/time stamp and Grants.gov Tracking number in an email serving as proof of their timely submission.

When DHS successfully retrieves the application from Grants.gov, and acknowledges the download of submissions, Grants.gov will provide an electronic acknowledgment of receipt of the application to the email address of the applicant with the AOR role who submitted the application. Again, proof of timely submission will be the official date and time that Grants.gov receives your application. Applications received by Grants.gov after the established due date for the program will be considered late and will not be considered for funding by DHS.

Applicants using slow internet, such as dial-up connections, should be aware that transmission can take some time before Grants.gov receives your application. Again, Grants.gov will provide either an error or a successfully received transmission in the form of an email sent to the applicant with the AOR role attempting to submit the application. The Grants.gov Support Center reports that some applicants end the transmission because they think that nothing is occurring during the transmission process. Please be patient and give the system time to process the application.

11. Content and Form of Application Submission

Applicant must submit all required documents listed in this section. See the Grants.gov Online Help for instructions on how to attach documents and complete forms. Applicant should ensure that the final submitted application package includes all required forms and documents.

Application Package

The following documents comprise, as applicable, the continuation/supplement package. Additional information regarding each of these documents is further provided.

a. Program Abstract
b. Program Narrative
c. Updated Plans to include:

1. Program Approach
2. Program Management Plan

d. Budget Narrative
e. Budget Forms updated as applicable: (Available on Grants.gov)
    1. Form SF-424, Application for Federal Assistance
    2. Form SF-424A, Budget Information for Non-Construction Programs
    3. Form SF-424B, Assurances for Non-Construction Programs
    4. Form SF-LLL, Disclosure of Lobbying Activities
f. Letters of Commitment
g. Draft Service Operational Plan

The Program Abstract, Program Narrative, Approach and Budget Narrative sections of the package must be double-spaced, on 8-1/2" x 11" plain white paper with 1" margins on all sides and use either Cambria or Times New Roman font size of not less than 11 points. Smaller font sizes may be used to fill in the Standard Forms, exhibits, and figures, though all text in forms, exhibits, and figures must not be smaller than 8-point font.

a. Program Abstract:
Recipient must include an abstract. This abstract is often distributed to the public and Congress and represents a high-level summary of the program. As a result, Recipient should prepare a clear accurate, concise abstract that can be understood without reference to other descriptions of the program, including: the program's mission, objectives, overall approach, and anticipated outcomes.

b. Program Narrative:
The program narrative provides the most substantive information regarding the proposed program in a clear and concise manner. To that end, the program narrative should address the elements articulated in the Program Description / Program Overview, Objectives and Priorities criteria presented in this NOFO. The program narrative should also align with the Performance Goals/Program Milestones and Performance Metrics presented in this NOFO.

c. **Program Approach:**
The Program Approach must be a clear and specific description of the Recipient's approach to build upon their organization's existing infrastructure in order to meet the objective of a streamlined cyber threat information sharing process that will allow the SLTT entity (foremost includes the critical subsector of Elections) to send cyber security threat information to a single entity and give that entity the responsibility to incorporate and integrate security orchestration, automation and response with other platforms and disseminate prioritized cyber information for the benefit of the entire SLTT sector on an equitable and timely basis.

Applicant should address the deployment of cyber managed services and use of the ISAC infrastructure to improve the sharing of cyber threat information amongst SLTT stakeholders to include:

i. The current infrastructure and resources that exist in their organization and how they will expand their infrastructure to achieve the proposed objectives and deliverables of the project.

ii. An assessment of the current state of the ISAC infrastructure's technical readiness and information sharing activities and a discussion that illustrates how they are applied to advance interoperable SLTT IT systems.

iii. Identification of strategies to implement cybersecurity managed services/tools and disseminate those tools to the SLTT sector.

iv. The workflow associated with the program and how the organizations involved in the program will be integrating information using resources from across the SLTT and federal government.

v. A description of how the applicant will use CISA funds in the next few years of the cooperative agreement to build additional SLTT subject matter threat modeling expertise and capacity for educational outreach to the SLTT sector; and

vi. A description of how the applicant will use additional threat information sources, provide technical capacity, to meet the objective to expand its capability to identify undetected threats, incorporate it into threat scoring, enable more automated defensive blocking

d. **Program Management Plan:**
Applicant is required to submit a Program Management Plan to CISA PO. The Project Plan must reflect, and be consistent with, the Program Narrative and Budget and must cover the duration of the projected period of performance. The Plan must also identify important objectives and deliverables associated with the Program, including:

i. The current infrastructure and resources that exist in their organization and how they will expand their infrastructure to achieve the proposed objectives and deliverables of the program.

ii. An assessment of the current state of the ISAC infrastructure's technical readiness and information sharing activities and a discussion to illustrate how they are applied to advance interoperable SLTT/Election's systems and cyber threat sharing.

iii. Identification of strategies to implement cybersecurity tools and disseminate those tools and services to the SLTT/Elections sector; and

iv. A sustainability plan that would allow for continuous sharing of cyber threat information.

The Program Management Plan must be broken out by each year and cover the duration of the cooperative agreement's projected period of performance. For each activity/objective, the cost will be projected. For each major task or action step within the activity, the plan must identify timeframes involved, including start and end dates. Upon award, CISA PO will provide feedback on the Program Management Plan and may request revisions before Program work can commence.

The Program Management Plan must include baseline measurements for each of the established milestone objectives. The applicant should propose performance metrics for how the applicant will measure its progress toward each objective. Metrics will include how the applicant would set goals and track progress on expanding its solutions over the phases of the award.

Applicant must, in their Program Management Plan, assess their current state of technical readiness and knowledge of the SLTT sector (includes critical sub-sectors, i.e., Elections) and demonstrate their understanding of the specific steps that need to be taken to meaningfully deliver robust solutions, protection and support, for SLTT members that range from small and medium to enterprise level organizations.

e. Budget Narrative/Justification

The Budget Narrative describes how the proposed budget, as articulated in the SF-424A, aligns with the applicant's Project Narrative to ensure that costs are realistic (not artificially too low) and reasonable (not inflated) in view of programmatic requirements.

When more than 33% of a Project's total budget falls under a contractual expense, a detailed Budget Narrative/Justification must be provided for each sub-contractor or sub-Recipient.

Whether direct or indirect, costs must be allowable, allocable, reasonable, and necessary under the applicable OMB Cost Circulars.

The period of performance for this award is 2 years. Recipient must submit a proposal which covers the full 2-year period. The budget and justification of costs should only include the initial 12-month budget period..

In subsequent years, Recipients will be able to revise their budgets, based on actual funding available from DHS, as part of their non-competing continuation

applications which will be required from all Recipients prior to the end of each budget period. The budget proposal must include:

i. An explanation of how the proposed budget supports the proposed Program and is reasonable to meet the Program's needs.
ii. How proposed costs support Program activities; and
iii. A description of how the proposed expenditures align with the Program Management Plan.

f. **Budget Forms:**
The Recipient is required to maintain the following budget forms to include the costs associated with the proposed Program activities. These forms are available and will be submitted/maintained through grants.gov as part of the application package and will include the following:

1.Application for Federal Assistance SF-424
2.Budget Information for Non-Construction Programs SF-424A
3.Assurances for Non-Construction Programs SF-424B
4.Disclosure of Lobbying Activities SF-LLL

i. **Form SF-424, Application for Federal Assistance**
Please note that the SF-424 is used for a wide variety of Federal grant programs and cooperative agreements, and Federal agencies have the discretion to require some or all the information on these forms.

ii. **Form SF-424A, Budget Information for Non-Construction Programs**
Please note that the SF-424A is used for a wide variety of Federal grant programs and cooperative agreements, and Federal agencies have the discretion to require some or all the information on these forms. All direct and indirect costs must be allowable, allocable, reasonable, and necessary.

iii. **Form SF-424B, Assurances for Non-Construction Programs**
This form contains laws and other assurances applicants must comply with under the discretionary funds programs administered by the DHS. Please note that a duly authorized representative of the applicant organization must certify that the organization is in compliance with these assurances.

iv. **Form SF-LLL, Disclosure of Lobbying Activities**
This form contains the name and address of lobbying registrants. Please note that a duly authorized representative of the applicant organization must sign the disclosure form. Failure to complete and sign the form may result in civil penalties ranging from $10,000 to $100,000.

g. **Letters of Commitment**

Include letters of commitment confirming support to the program (should it be funded) made by key collaborating organizations and agencies. Any organization that is specifically named to have a significant coordination role in carrying out a project should be considered an essential collaborator such as interstate, intrastate, and regional partners. At a minimum, the letter must explain the demonstrated commitment to the program and how they will advance coordination and collaboration among critical stakeholders.

Applicants will also provide a letter of commitment from entities that will be responsible for generating reports based on transactional data (e.g., internet service providers, technology vendors, or others). These entities should have the capacity and resources to produce required reports on adoption and use in a timely manner.

Signed letters of commitment should be scanned and included as attachments.

12. Other Submission Requirements

Transition Plan:
The Applicant must include a Transition Plan with its proposal for consideration during proposal evaluation. See Appendix A Task 1 for further information.

Draft Service Operational Plan, including:

a. Sustainability Planning section:
The Government is aware that, to be sustainable in the long-term, the Recipient must be able to build a business model to support its activities. Current organizations that are providing cyber threat information sharing services charge fees for services. The Recipient will not be expected to charge membership fees but should include a plan for sustainably providing some minimal level of threat information sharing services to the entire SLTT sector while building a plan for tiered services that would be available at additional fees to member organizations.

b. Service Operating Model section:
Clarify the basic structures, processes, and methods for delivering value to a diverse set of stakeholders (from small offices to large enterprise systems), with widely varying degrees of technical knowledge. The applicant must define how it will sustainably provide Cyber threat information to the entire SLTT sector, including how it will expand its cyber support and solutions to new SLTT organizations, what/if their fee structure will be for participation, what its expected baseline level of service will be to the entire sector, and how they will develop needs-based fee structures to assure all participants in the SLTT sector can use the baseline services offered.

c. Description of current services.

13. Intergovernmental Review *(Include if applicable)*

An intergovernmental review may be required. Applicants must contact their state's Single Point of Contact (SPOC) to comply with the state's process under Executive Order 12372.

14. Funding Restrictions

Applicants are advised of the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200.

DHS cooperative agreement funds may only be used for the purpose set forth in the cooperative agreement and must be consistent with the statutory authority for the award. Cooperative agreement funds and non-monetary support may not be used for matching contributions for other federal grants or cooperative agreements, lobbying, or intervention in federal regulatory or adjudicatory proceedings. Federal employees are prohibited from serving in any capacity (paid or unpaid) on any proposal submitted under this program. Federal employees may not receive funds under this award. In addition, federal funds may not be used to sue the Federal Government or any other government entity.

CISA PO substantial programmatic involvement and performance/progress reviews may result in funding restrictions in conjunction with the initial and continuation awards.

15. Allowable Costs

a. **Pre-Award Costs**
Pre-award costs incurred between the application start date and commencement of the budget period may be allowable if included in the application and approved by CISA in the Federal Award. To request pre-award costs, a written request must be included in the application that outlines what the pre-award costs are for, including a detailed budget breakdown of pre-award costs from the post-award costs and justification for approval.

b. **Management and Administration (M&A) Costs** *(if applicable)*
Recipient M&A costs are allowed for both the Recipient and subrecipients. A Recipient may use up to 5% of the federal award for M&A purposes. In addition, a subrecipient may use up to 5% of the amount they receive from the Recipient under a subaward for M&A purposes. M&A costs and activities are not operational costs; they are costs and activities incurred in direct support of the cooperative agreement or because of the cooperative agreement and should be allocated across the entire lifecycle of the cooperative agreement. They are directly related to managing and administering the federal award, such as financial management, reporting, and program and financial monitoring. It should be noted that salaries of a Recipient's personnel are not typically categorized as M&A costs unless the Recipient chooses to assign personnel to specific M&A activities.

c. Indirect Facilities and Administrative (F&A) Costs *(if applicable)*
Indirect Costs are allowable for the Recipient and any proposed subrecipient (if applicable). The applicant must attach a copy of the latest indirect cost rate agreement negotiated with a cognizant federal agency. If the applicant is in the process of initially developing or renegotiating a rate, upon notification that an award will be made, it should immediately develop a tentative indirect cost rate proposal based on its most recently completed fiscal year, in accordance with the cognizant agency's guidelines for establishing indirect cost rates and submit it to the cognizant agency. Applicants awaiting approval of their indirect cost proposals may also request indirect costs. When an indirect cost rate is requested, those costs included in the indirect cost pool should not also be charged as direct costs to the award. If the applicant is requesting a rate which is less than what is allowed under the program, the authorized representative of the applicant organization must submit a signed acknowledgement that the applicant is accepting a lower rate than allowed.

Any non-Federal entity that has never received a negotiated indirect cost rate (except for those non-federal entities described in Appendix VII to Part 200 States and Local Government and Indian Tribe Indirect Cost Proposals, paragraph D.1.b) may elect to charge a de minimis rate of 10% of modified total direct costs (MTDC) which may be used indefinitely. As described in 2 C.F.R. § 200.403 Factors Affecting Allowability of Costs, costs must be consistently charged as either indirect or direct costs but may not be double charged or inconsistently charged as both. If chosen, this methodology once elected must be used consistently for all federal awards until such time as a non-federal entity chooses to negotiate for a rate, which the non-federal entity may apply to do at any time. For more information, see 2 C.F.R. § 200.414.

E. Application Review Information

1. Application Evaluation Criteria

a. Programmatic Criteria

DHS will evaluate applications deemed eligible against the criteria set forth below.

Factor 1: Technical (Maximum of 45 Points)

Sub-factor 1.1 Indicator-to-action workflow planning, design, and execution (Maximum of 20 Points)

Sub-factor 1.2 Systems Engineering and Integration (Maximum of 10 Points)

Sub-factor 1.3 Capacity for secure Automated Indicator Handling (Maximum of 10 Points)

Sub-factor 1.4: Bidirectional Sharing capabilities and integration (5 Points)

Factor 2: Business Management (Maximum of 35 Points)

Sub-factor 2.1 Overall business management approach in providing cybersecurity operational services that protect SLTT (Maximum of 15 Points)

Sub-factor 2.2 Personnel Management & Retention (Maximum of 10 Points)

Sub-factor 2.3 SLTT (and Elections) Outreach and Communications (Maximum of 10 Points)

Factor 3: Past Performance and Prior Experience (Maximum of 10 Points)

Factor 4: Effectiveness & Cooperative Agreement Cost Share Methodology (Maximum of 10 Points)

Relative Order of Importance

Factor 1 (Technical) is more important than Factor 2 (Management). Factor 2 (Management) is more important than Factor 3 (Past Performance). Factor 3 (Past Performance) is more important than Factor 4 (Cost Effectiveness). Factors 1-3 (Technical, Management, Past Performance) are significantly more important than Factor 4 (Cost Effectiveness).

Factor 1- Technical

Capabilities Demonstration

The applicant must conduct a Capabilities Demonstration to evaluate how the applicant's solution meets the workflow functionality as well as technical requirements of this award. During the demonstrations, applicants will be evaluated on their maturity model to meet CISA PO defined functional and technical capabilities. In addition, the demonstrations will provide input for assessing related criteria and validating the overall approach. The extent to which the applicant demonstrates:

1.1 Indicator-to-action workflow planning, design, and execution

- Applicant agility in implementing workflow processes that share prioritized cyber threat information amongst community members to protect from and/or mitigate the threat at expedited speed.

1.2 Systems Engineering and Integration

• Approach and methodology for managing, expanding, enhancing, storing, integrating, and sharing threat data and information. The approach must include updating architecture hardware and software assets to support innovative technology and/or new capabilities insertion.

• Description for how applicant's systems engineering approach and methodology supports maintaining the overall security posture and maintaining enterprise-wide configuration management, problem, and release management.

• Approach, methodology, capabilities, and capacity of proposed staffing

1.3 SOC operating capabilities

• Security Information and Event Management optimization for near real time event collection and analysis

• Use big data optimization capabilities to analyze unique ISAC sources of data, including but not limited to Albert network data, to conduct pattern and statistical analysis to detect outliers and unusual behaviors.

• Threat Intelligence Security Tool Alerting optimization

• Ability to add time to SOC analyst through automation of repetitive activities

1.4 Bidirectional Sharing capabilities and integration

• Demonstrate the ability and preference to foster and encourage bidirectional sharing between CISA and SLTT entities.

Factor 2: Business Management

The Government will evaluate the Applicant's:

2.1 Overall Business Management approach in providing cybersecurity operational services

• Approach to meeting SLTT national cybersecurity resilience capability objectives — such as information sharing, risk mitigation, incident response, engagement, and workforce development.

2.2 Key Personnel Management & Retention

• Approach to provide a sound key personnel management strategy to include recruiting and hiring key personnel; and retaining capable, qualified, and skilled key personnel.

2.3 SLTT (and Elections) Outreach and Communications Plan

• Outline of activities/communications that will be done to communicate strategy and move SLTT stakeholders to accomplish goals.

Factor 3: Past Performance and Prior Experience

3.1 Assesses the degree of confidence the Government has in an Applicant's ability to deliver capabilities and services that meet the cybersecurity efforts at hand based on a demonstrated record of performance. The Government will evaluate the relevancy, recency, and overall performance confidence in the Applicant's past performance.

Factor 4: Effectiveness & Cooperative Agreement Cost Share Methodology

4.1 The extent to which the applicant's proposed budget shows an effective use of cooperative agreement funds.

4.2 Approach to managing program cost, schedule, and technical performance

4.3 Approach to managing SLTT partner paid delivery of service through crowdsourced pricing policies to support members who may lack resources for obtaining cybersecurity tools.

b. **Financial Integrity Criteria**

Prior to making a federal award, the DHS FAO is required by the Payment Integrity Act of 2019, 41 U.S.C. §2313 – Database for federal agency contract and grant officers and suspension and debarment officials, and 2 C.F.R. § 200.206 to review information available through any OMB-designated repositories of government wide eligibility qualification or financial integrity information. Therefore, application evaluation criteria may include the following risk-based considerations of the applicant:

1) Financial stability.
2) Quality of management systems and ability to meet management standards.
3) History of performance in managing federal award.
4) Reports and findings from audits.
5) Ability to effectively implement statutory, regulatory, or other requirements.

c. **Supplemental Financial Integrity Criteria and Review**

Prior to making a federal award where the anticipated total federal share will be greater than the simplified acquisition threshold, currently $250,000 (see Section 805 of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, OMB Memorandum M-18-18 at https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-18.pdf):

1) GFAD is required to review and consider any information about the applicant that is in the designated integrity and performance system accessible through SAM, which is currently the Federal Awardee Performance and Integrity Information System (FAPIIS) and is accessible through the sam.gov website.

2) An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.

3) GFAD will consider any comments by the applicant, in addition to the other information in FAPIIS, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in 2 C.F.R. §200.206.

2. Review and Selection Process

The review and selection process are designed to ensure that cooperative agreement applications are evaluated based on a fair, equitable, transparent, bias-free, and timely process, and that awards align with the selection criteria, priorities, and strategic considerations stated in this Notice.

DHS uses a multi-stage process to review and assess applications. Reviewers read, assess, discuss, and provide feedback on the application. The results of the review are compiled and analyzed and used to inform DHS's subsequent decision-making process and to clarify requirements for continuation applications.

The main offices involved in the cooperative agreement application review and selection process are:

- CISA Cybersecurity Division (CSD) Joint Cyber Defense Collaborative (JCDC) – owns the cooperative agreement competition and participates in each step of the application review, recommendation, and decision-making process. Office of the CSD Executive Assistant Director – provides strategic direction and makes final funding decisions.

- CISA Stakeholder Engagement Division (SED) Strategic Relations - participates in each step of the application review, recommendation, and decision-making process.

- CISA National Risk Management Center (NRMC) Elections Infrastructure Security Office- participates in each step of the application review, recommendation, and decision-making process.

- Grants and Financial Assistance Division (GFAD) – provides budget and financial reviews of grant and cooperative agreement applications and makes the actual award.

- DHS Office of the General Counsel (OGC) and CISA Office of the Chief Counsel (OCC)– provide legal counsel to DHS and CISA.

CISA will conduct an initial review of applications to determine the responsiveness of the application. If an applicant is determined to be ineligible (see Section C. Eligibility Information) or an application is determined to be non-responsive, DHS will notify the applicant. All responsive and eligible applications will be reviewed as described below:

1. CISA PO will assemble a review panel which may include both federal employees and subject matter experts (non-federal reviewers) to review the eligible applications. Reviews of submitted applications will be conducted either on site or by remote review.

2. Technical reviewers will review each eligible application against the evaluation criteria. The reviewers will assign a score and provide summary comments based on the evaluation criteria identified above.

3. An application may be selected for a post-review quality control and possible rescoring if it received significantly diverging scores and comments from reviewers.

4. An internal review panel consisting of CISA staff will review the highest ranked applications and make final funding recommendations. The internal review panel may take applications out of rank order in consideration of strategic program priorities, which are identified below.

5. CISA may perform an additional review of the applicant organization and any and/or its key personnel. This may include reviewing audit reports, publicly available materials and/or government databases and may have a bearing on award outcome. DHS may request additional materials from the applicant as part of this review, including:

- The summary letter from the applicant's most recent audit report; and
- Documentation of previous cooperative agreement completion that includes the name of the Recipient, amount awarded, and whether the Recipient sufficiently completed the requirements of the cooperative agreement (e.g., a final close-out report, certification of completion, etc.)

6. After the technical review and before making final funding decisions, CISA may contact the highest-ranking applicants to seek clarification and to discuss technical and programmatic aspects of the application. If an application includes a subrecipient, CISA may request to speak with all parties included in the application to ensure sufficient planning and coordination has taken place prior to making an award.

7. **Confidentiality and Conflict of Interest**. Technical and cost proposals submitted under this funding opportunity will be protected from unauthorized disclosure in accordance with applicable laws and regulations. CISA may use one or more support contractors in the logistical processing of proposals. However, funding recommendations and final award decisions are solely the responsibility of CISA personnel.
   CISA screens all technical reviewers for potential conflicts of interest. To determine possible conflicts of interest, CISA requires potential reviewers to complete and sign conflicts of interest and nondisclosure forms. CISA will keep the names of submitting institutions and individuals as well as the substance of the applications confidential except to reviewers and CISA staff involved in the award process to the extent consistent with applicable law. CISA will destroy any unsuccessful applications after three years following the funding decision.

8. CISA strongly discourages, and will not consider, any materials submitted by or on behalf of the applicant (e.g., letters of support) other than those materials specifically requested in this NOFO.

9. The designated selection authority will make a final award decision using input from the review panel.

10. CISA will notify all applicants electronically of funding decisions. Unfunded applicants may send a written request to the DHS Grants Officer, shareef.prater@hq.dhs.gov to receive a debriefing. Additional information beyond that described here will not be provided.

F. Federal Award Administration Information

1. Notice of Award

Before accepting the award, the AOR and Recipient should carefully read the award package. The award package includes instructions on administering the cooperative agreement and the terms and conditions associated with responsibilities under federal awards. By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

A cooperative agreement will be executed by a DHS Grants Officer authorized to obligate CISA funding. The notice of federal award will be signed by the DHS Grants Officer and provided to the Recipient via electronic means.

2. Pass-Through Requirements *(if applicable)*

1) The Recipient must store and make readily available for CISA to unilaterally access any continuous monitoring data for contractor and subcontractor systems used in performance of the Cooperative Agreement (CA) for a period not less than one year from the date the data is created. "Continuous monitoring data" includes, but not limited to, logs addressing authentication, mailbox, and folder changes (including deletion), rule creation and deletion, secondary application access and changes, user creation and deletion, and administrator actions. The Recipient must insert a clause containing all the provisions of this clause, including this paragraph, in all subcontracts expected to create, archive, or store continuous monitoring data.
2) The Recipient or subcontractor of systems used in performance of the agreement, must permit, at CISA's election, CISA to (1) perform continuous monitoring and IT security scanning from Government tools and infrastructure or (2) direct performance of continuous monitoring and IT security scanning from tools that are provided by the Recipient or otherwise found within the Recipient's environment. The Recipient must insert a clause containing all the provisions of this clause, including this paragraph, in all subcontracts for systems used in performance of the Cooperative Agreement.
3) The Recipient must comply with the timelines and substantive requirements applicable to agencies in the Federal Incident Reporting Requirements (FIRR) and successor documents for any incidents involving Recipient or subcontractor systems used in performance of the CA. The Recipient must insert a clause containing all the provisions of this clause, including this paragraph, in all subcontracts for systems used in performance of the CA.
4) The Recipient must, at CISA's election, permit CISA to deploy and maintain a cyber threat hunting capability to search for indicators of compromise in any Recipient or subcontractor systems used in performance of the cooperative agreement and detect, track, and disrupt threats that evade existing controls. The Recipient must insert a clause containing all the provisions of this clause, including this paragraph, in all contracts for systems used in performance of the CA.

5) The Recipient must share cyber threat indicators (as defined at 6 U.S.C. § 1501(6)) with any and all available associated context and defensive measures (as defined at 6 U.S.C. § 1501(7)) in an automated fashion using CISA's Automated Indicator Sharing (AIS) platform or successor technology for mitigated and non-mitigated events with a cyber nexus.
6) The Recipient must comply with and, in accordance with reporting requirements levied on Federal agencies and at CISA's request, provide a report on compliance with Federal mandates to include Binding Operational Directives and Emergency Directives. The Recipient must provide CISA with the report by the date required in the mandate (unless otherwise requested by CISA) and include a statement regarding the Recipient's approach to implementing the mandate (e.g., the mandate has been implemented, or a compensating control or other mitigation is in place.)
7) The Recipient must provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response. For all Recipient or contractor systems used in performance of the CA, this includes access to administrative networks, systems, and accounts; access to underlying infrastructure systems; and all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. Activities may include inspections, investigations, forensic reviews, and data analyses and processing. The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities. The Recipient must insert a clause containing all the provisions of this clause, including this paragraph, in all contracts for systems used in performance of the CA.

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

provisions of this clause, including this paragraph, in all contracts for systems used in performance of the cooperative agreement.

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

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

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

- ED 22-03 - Mitigate VMWare Vulnerabilities
- ED 22-02 - Mitigate Apache Log4J Vulnerability (Closed)
- ED 21-04 - Mitigate Windows Print Spooler Service Vulnerability
- ED 21-03 - Mitigate Pulse Connect Secure Product Vulnerabilities
- ED 21-02 - Mitigate Microsoft Exchange On-Premises Product Vulnerabilities
- ED 21-01 - Mitigate SolarWinds Orion Code Compromise
- ED 20-04 - Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday
- ED 20-03 - Mitigate Windows DNS Server Vulnerability from July 2020 Patch Tuesday
- ED 20-02 - Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday
- ED 19-01 - Mitigate DNS Infrastructure Tampering
- BOD 23-01 - Improving Asset Visibility and Vulnerability Detection on Federal Networks (BOD 23-01 - Implementation Guidance)
- BOD 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities
- BOD 20-01 - Develop and Publish a Vulnerability Disclosure Policy
- BOD 19-02 - Vulnerability Remediation Requirements for Internet-Accessible Systems

- BOD 18-02 - Securing High Value Assets
- BOD 18-01 - Enhance Email and Web Security
- BOD 17-01 - Removal of Kaspersky-branded Products
- BOD 16-03 - 2016 Agency Cybersecurity Reporting Requirements
- BOD 16-02 - Threat to Network Infrastructure Devices

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

3. Administrative and National Policy Requirements

All successful applicants for DHS grants and cooperative agreements are required to comply with DHS Standard Terms and Conditions, which are available online at: DHS Standard Terms and Conditions.

The applicable DHS Standard Terms and Conditions will be those in effect at the time the award was made unless the application is for a continuation award. In that event, the terms, and conditions in effect at the time the original award was made will generally apply. What terms and conditions will apply for the award will be clearly stated in the award package at the time of award.

By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

a. **Non-Disclosure Requirements**

The federal award may require the Recipient to have access to information relating to any and all aspects of cooperative agreement operations that may be of a technical, legal, sensitive and/or confidential nature and which may be the sole property of the U.S. Government. To mitigate risks associated with such access, the Recipient must ensure that all its personnel, including chief executives, directors, consultants, sub Recipients, or any other personnel substantially involved in the performance of this award sign a non-disclosure agreement prior to the commencement of any work on the award.

In addition, Recipients must put in place appropriate procedures for the protection of such information and will be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel.
The rights and remedies of the Government, under this term and condition, will not be exclusive and are in addition to any other rights and remedies provided to the Government under law, regulation, or any other available enforcement mechanism.

4. Reporting

1) Federal Financial Reporting Requirements

i. Financial Reporting Accounting - the Recipient must provide a clear composition of their spending within the core services, shared services/required functionalities, and programs. The clear breakdown of these funds should be applied to the following, but not be limited to: In-Progress Reviews (IPRs), Program Management Reviews (PMRs), ABC reports, Quarterly Federal Financial Reports, Semi-Annual Federal Financial Reports, Final Federal Financial Reports. The Recipient must work with the PO to define an agreed-upon template for reporting fiscal year's financial breakdowns that will include at minimum cumulative expenditures, monthly expenditures, and monthly forecasts.

ii. The Federal Financial Report (FFR) form is available online at: SF-425 *OMB #4040-0014.*

iii. Semi-Annual Federal Financial Reports - Expenditures must be reported, on a semi-annual basis, using the SF-425, Federal Financial Report (FFR). Recipients must submit reports to DHS no later than April 30 of each year the award is active for funds expended between October and March, and no later than October 31 for funds expended between April and September. The semi-annual FFR will be submitted electronically via www.GrantSolutions.gov.

iv. Quarterly Federal Financial Reports (Cash Transaction) - The FFR Cash Transaction Report, a subset of the SF-425, Federal Financial Report, is submitted via the Payment Management System (PMS) every calendar quarter for the life of the award. The report must be submitted within 30 days after the end of the quarter (no later than January 31, April 30, July 31, and October 31).

v. Monthly Financial Activity-Based Costing (ABC) Report
CISA PO will provide a formatted template for an activity-based costing model that identifies program activities. The Recipient will then assign the cost of each activity with resources to all program services and according to the actual consumption by each. CISA PO reserves the right to amend the format as necessary. Activity Reports will be delineated by fixed/variable cost drivers that define logical elements of capability. Report will include, but not be limited to: Funding Burn Rates, Partner-paid cost share, Budget Forecast, Estimate At Completion (EAC), Budget vs EAC variance. ABC Reports shall be submitted along with IPR materials each month. Reports shall be emailed to the CISA PO at CISA.CSD.JCDC_MS-ISAC@cisa.dhs.gov and uploaded to the GrantSolutions system, using the

Grant Note feature. Guidance is found here: https://www.grantsolutions.gov/support/granteeUsers.html

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

2) Programmatic Performance Reporting Requirements

i. Quarterly Performance Reports - the Recipient must submit performance reports to the DHS/CISA Grants Officer no later than 30 days after the end of the reporting period end date. Reports are due on the following dates: 01/31, 04/30, 07/31 and 10/31. The report must be submitted via GrantSolutions using the Help/Support Reference entitled, Grant Recipient Process: Performance Progress Reporting.

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

- A summary that clearly differentiates between activities completed under the SLTT SOC|ISAC cooperative agreement and related activities completed with other sources of leveraged funding.
- Performance Metric Reporting as outlined in Appendix A Task 10.
- A summary and status of approved activities performed during the reporting period; a summary of the performance outputs/outcomes achieved during the reporting period; and a description of problems encountered during the reporting period that may affect the project schedule.
- A comparison of actual accomplishments with the goals and objectives established for the period in the DHS/CISA-approved workplan.
- Difficulties encountered and reasons why established objectives were not met, if applicable.
- An update on project schedules and milestones, including an explanation of any discrepancies from the DHS/CISA-approved workplan.
- A discussion of expenditures and financial status for each workplan task, along with a comparison of the percentage of the project completed to the project schedule and an explanation of significant discrepancies shall be included in the report.
- A budget recap summary table with the following information: current approved project budget; DHS/CISA funds drawn down during the reporting period; costs drawn down to date (cumulative expenditures); program income generated and used (if applicable); and total remaining

funds.
- Other pertinent information including, when appropriate, any discrepancies in the budget from the DHS/CISA-approved workplan, analysis and explanation of cost overruns or high unit costs.
- For the quarterly performance reports, provide a high-level comparison between the last quarterly report and the current reporting period.
- At the end of the fourth quarter provide both a fourth quarter performance report and an Annual Summary Performance Report.

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

ii. In accordance with 2 C.F.R. § 200.329(e)(1), the Recipient will inform DHS/CISA via email, as soon as problems, delays, or adverse conditions become known which will impair the ability to meet the outcomes specified in the DHS/CISA-approved workplan.

iii. Final Performance Report - the Recipient must submit the Final Performance Report to the DHS Grants Officer no later than 90 days after the expiration of the Project Period. The report must be submitted via GrantSolutions using the Grant Note submission guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

3) Additional Performance Reporting Requirements

Refer to Appendix A for additional reporting requirements.

4) Closeout Reporting Requirements

Within 120 days after the end of the period of performance, or after an amendment has been issued to close out a cooperative agreement, Recipients must submit the following:
1) The final request for payment, if applicable.
2) The final FFR (SF-425).
3) The final progress report detailing all accomplishments.
4) A qualitative narrative summary of the impact of those accomplishments throughout the period of performance; and,
5) Other documents required by this NOFO, terms and conditions of the award, or other GFAD guidance.

If applicable, an inventory of all construction projects that used funds from this program must be reported with the final progress report.

After these reports have been reviewed and approved by GFAD, a closeout notice will be completed to close out the cooperative agreement. The notice will indicate the period of performance as closed, list any remaining funds that will be de-obligated, and address the requirement of maintaining the cooperative agreement records for three years from the date of the final FFR, unless a longer period applies, such as due to an audit or litigation, for equipment or real property used beyond the period of performance, or due to other circumstances outlined in 2 C.F.R. §200.334, Retention Requirements for Records.

In addition, any Recipient that issues subawards to any subrecipient is responsible for closing out those subawards as described in 2 C.F.R. §200.344, Closeout. Recipients acting as pass-through entities must ensure that they complete the closeout of their subawards in time to submit all necessary documentation and information to GFAD during the closeout of their cooperative agreement.

The Recipient is responsible for returning any funds that have been drawn down but remain as unliquidated on Recipient financial records.

5) Disclosing Information per 2 C.F.R. § 180.335

This reporting requirement pertains to disclosing information related to government-wide suspension and debarment requirements. Before a Recipient enters into a cooperative agreement with GFAD, the Recipient must notify GFAD if it knows if it or any of the Recipient's principals under the award fall under one or more of the four criteria listed at 2 C.F.R. § 180.335:

1) Are presently excluded or disqualified.
2) Have been convicted within the preceding three years of any of the offenses listed in 2 C.F.R. § 180.800(a) or had a civil judgment rendered against it or any of the Recipient's principals for one of those offenses within that time period.
3) Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses listed in 2 C.F.R. § 180.800(a); or,
4) Have had one or more public transactions (federal, state, or local) terminated within the preceding three years for cause or default.

At any time after accepting the award, if the Recipient learns that it or any of its principals falls under one or more of the criteria listed at 2 C.F.R. § 180.335, the Recipient must provide immediate written notice to GFAD in accordance with 2 C.F.R. § 180.350.

6) Reporting of Matters Related to Recipient Integrity and Performance

Per 2 C.F.R. Part 200, Appendix I § F.3, the additional post-award reporting requirements in 2 C.F.R. Part 200, Appendix XII may apply to applicants who, if

upon becoming Recipients, have a total value of currently active grants, cooperative agreements, and procurement contracts from all federal awarding agencies that exceeds $10,000,000 for any period during the period of performance of an award under this funding opportunity. Recipients that meet these criteria must maintain current information reported in FAPIIS about civil, criminal, or administrative proceedings described in paragraph 2 of Appendix XII at the reporting frequency described in paragraph 4 of Appendix XII.

7) Monitoring and Oversight

Per 2 C.F.R. § 200.329, DHS, through its authorized representatives, has the right, at all reasonable times, to conduct desk reviews, make site visits to review project accomplishments and management control systems to review project accomplishments and to provide any required technical assistance. During site visits, DHS will review Recipients' files related to the cooperative agreement. As part of any monitoring and program evaluation activities, Recipients must permit DHS, upon reasonable notice, to review cooperative agreement -related records and to interview the organization's staff and contractors regarding the program. Recipients must respond in a timely and accurate manner to DHSrequests for information relating to the cooperative agreement**.**

8) Program Evaluation

Recipients and subrecipients are encouraged to incorporate program evaluation activities from the outset of their program design and implementation to meaningfully document and measure their progress towards the outcomes proposed Title I of the Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act), Pub. L. No. 115-435 (2019) defines evaluation as "an assessment using systematic data collection and analysis of one or more programs, policies, and organizations intended to assess their effectiveness and efficiency." Evidence Act § 101 (codified at 5 U.S.C. § 311). Credible program evaluation activities are implemented with relevance and utility, rigor, independence and objectivity, transparency, and ethics (OMB Circular A-11, Part 6 Section 290).

Evaluation costs are allowable costs (either as direct or indirect), unless prohibited by statute or regulation, and such costs may include the personnel and equipment needed for data infrastructure and expertise in data analysis, performance, and evaluation. (2 C.F.R. §200).

In addition, Recipients are required to participate in a DHS-led evaluation if selected, which may be carried out by a third-party on behalf of the Program Office or DHS. By accepting cooperative agreement funds, Recipients agree to participate in the evaluation, which may include analysis of individuals who benefit from the cooperative agreement, and provide access to program operating personnel and participants, as specified by the evaluator(s) during the award.

G. DHS Awarding Agency Contact Information

a. **Contact and Resource Information**

The Grants Officer for this award is:

Shareef Prater
Grants and Financial Assistance Division
Phone: 202-770-4776
Email: shareef.prater@hq.dhs.gov

The Program Manager for this award is:

Amy Nicewick
Cybersecurity and Infrastructure Security Agency
703-203-0634
Email: amy.nicewick@cisa.dhs.gov

The Telephone Device for the Deaf (TDD) and/or Federal Information Relay Service (FIRS) number available for this Notice is:

1-800-518-4726 (Grants.gov Help Desk)

b. **Systems Information**
N/A

H. Other Information

a. **Period of Performance Extensions**
Extensions to this program are allowed. Applicants may request a no-cost extension to complete all project activities. The request must be submitted 60 days prior to the expiration of the performance period. Requests for extensions are subject to approval by DHS.

b. **Other Information**

a. **Prior Approval**
The Recipient must 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.

b. **Budget Revisions**
Transfers of funds between direct cost categories in the approved budget when such cumulative transfers among those direct cost categories exceed ten percent of the total budget approved in this Award require prior written approval by the DHS Grants Officer.

i. The Recipient must obtain prior written approval from the DHS

Grants Officer for any budget revision that would result in the need for additional resources/funds.

ii. 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.

c. **Program Income**
A recipient must seek prior written approval from the DHS Grants Officer before the recipient or any subrecipient may earn program income under the Award during the Period of Performance. As defined by 2 C.F.R. § 200.1, program income means gross income earned by a non-federal entity that is directly generated by a supported activity or earned as a result of the Award during the Period of Performance. If approving the request, the DHS Grants Officer will identify whether the recipient may use the program income under the deduction, addition, or cost-sharing approach set forth at 2 C.F.R. § 200.307(e).

d. **Appendix A** (see attached)

e. **Appendix B** (see attached)

State, Local, Tribal and Territorial (SLTT)

Security Operations Center (SOC) | Information Sharing and Analysis Services (ISAC)

Program Work Supplemental Scope – Appendix A

Table of Contents

1 Purpose

The State, Local, Tribal, and Territorial (SLTT) community has diversified cybersecurity maturity levels across the community. The purpose of this Scope of Work (SOW) is to advance managed service capabilities and hasten establishment of an integrated national SLTT ecosystem approach, including the Elections Subsector. As requested by CISA Program Officer (PO), the Information Sharing Analysis Center (ISAC) managed security service efforts will be executed in order to provide the SLTT community with solution expertise, and simplify security operations with continuous, value-driven monitoring and management of cyber risk. Additionally, to help address complex SLTT enterprise management of risk, the Recipient will mature its own infrastructure capacity through innovative solutions that provide security automation, correlation, orchestration, and integration of intelligence across a Threat Intelligence Platform that provides a collaborative link to the SLTT community for rapid rollout resilience.

By technically integrating indicator context, providing analytic collaboration across the SLTT cyber community, empowering SLTT cyber expertise, and increasing situational awareness across the SLTT trusted membership circle, the community will collaboratively serve together to protect and improve defenses for the nation's SLTT and its critical infrastructure sub-sectors.

Furthermore, the Recipient will consistently engage with external partners including federal government, law enforcement, vendor community, and other ISACs and associations to integrate cyber situational awareness and will expand upon and leverage the existing capabilities of the participating Department of Homeland Security (DHS) / Cybersecurity and Infrastructure Security Agency (CISA) offices. This will create an even more robust and informed cyber information sharing environment for the benefit of the entire SLTT sector and its critical subsectors on an equitable and timely basis.

The SLTT trusted community focus on sharing timely, actionable, and relevant cyber information with each other across a Threat Intelligence Platform will improve the overall cybersecurity posture of the nation's SLTT governments. The gradual evolution of partnerships is envisioned to establish a circle of trust that supports a more complete and accurate picture of homeland defense, improves cyber technical expertise, and prevents malicious cyberspace actors and activities by defending forward, with the potential to become a significant enabler of improved resilience for the SLTT sector.

1.1 Objectives

The objectives of this SOW are to expedite building an automated and streamlined capacity to share cyber threat intelligence across a platform bi-directionally and collaboratively amongst the SLTT (to include the Elections Subsector) and CISA. It will also provide a mechanism for rapid adoption and methods to integrate with local activities in the SLTT enterprise/environment that improve cybersecurity awareness and equip stakeholders to act in response to

prioritized cyber threat intelligence shared within the threat intelligence platform. Furthermore, this effort will expand exploration of cyber managed services (e.g., National Prevention Program, Endpoint Detection and Response, Malicious Domain Blocking and Reporting) to include the Elections subsector, and in doing so will impact the capabilities to create a more robust cyber defense and information sharing environment for the entire SLTT sector.

This SOW is intended to fill a gap in services by providing supplemental resources to enable innovation, broaden centralized access to a cyber threat intelligence platform, provide for cyber workforce development, and enhance cyber readiness and resilience all while connecting the cyber ecosystems of the SLTT and Elections communities. By providing these funds, technical assistance, and access to federal resources, it is expected that the Recipient will be able to:

1) Conduct cyber threat intelligence enrichment, scoring and dissemination based on Indicators of Compromise (IOC) scoring derived from SLTT infrastructure, ISAC information sources, open-source, and external intelligence enrichment to include:
    - Enhance automation of existing processes and procedures to curate and disseminate a threat feed that aligns with a novel release/scoring methodology
    - Correlate new information sources to support implementation of threat scoring
    - Enrich ISAC analyst tickets and threat indicator databases with information derived during the scoring process
2) Create a lower entry cost for SLTT organizations (including elections infrastructure) who need help in managing cyber defenses and risk to include:
    - Identify and mitigate threat on SLTT premises, in the cloud, across the wire, and on remote systems
    - Continuation of Endpoint Detection and Response, Malicious Domain Blocking and Reporting, and using traffic aggregation
3) Expand the trusted SLTT community base that shares threat intelligence to include:
    - Maintain 24x7x365 security operations center (SOC) to drive bi-directional cyber threat sharing among multi-tenant SLTT communities of trust
    - Increase adoption of the Threat Intelligence Platform through promotional advertising and training
4) Provide some level of free managed security services and cyber threat intelligence sharing services to the SLTT sector, to include:
    - Implementing a Service Operational Plan that includes sustainment plans.

1.2 Assumptions and Constraints

This section defines the broad assumptions and constraints which the Recipient

must consider in developing its technical solution. Task specific assumptions and constraints are included within each functional task as applicable.

- Services must be consistent with industry best practices for Technical Reference Model (TRM) and Systems Engineering Life Cycle (SELC) Management.
- Solutions must utilize National Information Assurance Partnership (NIAP) protection profiles for intrusion detection systems, sensors, scanners, and analyzers, published by the U. S. National Security Agency Science Applications International Corporation. The Protection Profiles are compliant with Common Criteria. The Common Criteria is an international standard that specifies the criteria for security evaluation of IT hardware and software products.
- Services must comply with the Federal Information Security Modernization Act (FISMA). All hardware, software, and services provided under this Award must comply with the standards set forth in the National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171), "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."
- The Recipient must support the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 including, but not limited to the following elements:
    - Security Plan
    - Security Risk Assessment
    - Security Controls Assessment
    - Continuity of Operations Plan (COOP)
    - Development of POA&M

2 Referenced Documents

Specific DHS generated documents, policies, and procedures may contain sensitive information and will be made available to the Recipient for viewing but will not leave DHS infrastructure and/or facilities, be photocopied, or pen copied verbatim.

All internal CISA processes and procedures are based on industry standard best practices and have been customized to meet specific DHS requirements. Referenced documents include escalation procedures, standard operating procedures (SOP), and cyber exercise techniques.

The Recipient must control and safeguard For Official Use Only (FOUO) information in accordance with the most current version of DHS Management Directive (MD 11042.1) *Safeguarding Sensitive But Unclassified (SBU) Information*.

Classified information is Government information, which requires protection in accordance with Executive Order 13526 National Security Information (NSI) as amended and supplemental directives.

3 Scope of Work

The SOW consists of support tasks and duties needed to support a robust cyber-Indications and Warning (I&W) program that moves capability from manual messaging toward a means for convening SLTT governments to connect cyber ecosystems, identify cyber threat adversary action and enable automated ways to export and integrate intelligence for proactive implementation of countermeasures to mitigate or minimize impact. This will help connect the trusted SLTT community to coordinate resilience efforts and provide an I&W communications infrastructure for the benefit of all.

Successful execution of this SOW will focus on new models for sharing threat intelligence, integration of computational and automated methods into user-driven analytic techniques, and incorporation of collaborative means for analysts within the operational SLTT community to help provide warning of an imminent malicious cyber scenario and decrease time to mitigation.

Building indicator context and expanding cyber expertise amongst the SLTT community assists CISA and Federal partners to establish, enable, and analyze measures that will help ensure the security of the Nation's broad and interdependent cyber infrastructure.

Recipient must ensure all programs are operational within 12 months of Award. This includes all Proofs of Values reports completed and programs are in an operational state.

A "program" is any activity or group of activities that falls within this Scope of Work.

Program Goals and Milestones

The CISA PO establishes program priorities that represent overarching goals for the SLTT SOC|ISAC Cooperative Agreement. In keeping with the objectives of this Cooperative Agreement, CISA PO will target funding toward activities within the SLTT sector related to increasing knowledge and understanding of cybersecurity threats and how to address them. The projects and deliverables outlined in these appendices are subject to change. The Recipient must also work closely with the DHS and CISA support offices. The Recipient will benefit from the information CISA will provide in support of the Cyber mission. CISA will provide analysis and context to CISA-supplied information, synthesizing it with information obtained from other sources, and developing explanatory insights with recommendations for threat mitigation. The Recipient must prioritize service deployment and delivery to specific, identified entities when determined by CISA PO and as result of CISA intelligence priority schemas.

Structure and Approach

The SOW is comprised of 41 tasks that are divided into the following functional

areas:

1. Functional Area 1 – Program Management
2. Functional Area 2 – Cybersecurity Operations Center
3. Functional Area 3 – SOC Architecture, Engineering, Service Delivery, and Maintenance
4. Functional Area 4 – Cybersecurity Communications and Coordination

4 Program Components/Priorities

4.1 Functional Area 1: Program Management

4.1.1 Task 1 – Transition

The Recipient will assume responsibility for carrying out the scope of work from the incumbent Recipient, if applicable, without degradation of service upon Award.

Within 30 days of Award, the Recipient must provide an orientation to introduce CISA personnel, programs, and users to the Recipient leadership and services team, tools, methodologies, business processes, etc.

The Recipient must support the CISA PO to coordinate any required transition actions and services handoffs associated with meeting the transition completion deadline. This includes, but is not limited to, the following:

1. Review, evaluation, and transition of incumbent support services
2. Transfer and update Government-approved incumbent training and processes
3. Transfer of all necessary incumbent procedural and technical documentation
4. Transfer of incumbent Government Furnished Equipment (GFE) and Government Furnished Information (GFI) and Data to the Recipient, as appropriate
5. Inventory management and inventory reporting for all GFE assigned to the SLTT community

The Recipient must develop a Transition Plan that specifies the steps the Recipient will take to provide for the orderly transition of support services from the incumbent. The Recipient must include this Transition Plan with its proposal for consideration during proposal evaluation.

Within 10 days of Award, the Recipient must update the Transition Plan originally submitted with Recipient's Proposal to address comments and direction, if any,

provided by the DHS CISA PO.

The Recipient's Transition Plan must address, at a minimum, the following elements:

1. A work plan that defines a phased transition approach, including descriptions of specific transition tasks and task completion dates, and demonstrates how the Recipient will conclude the transition within sixty (60) calendar days after task order Award.
2. Schedule in graphic format showing the timing, sequence, and interdependencies of transition tasks.
3. Clear entry and exit criteria for each task transitioned from the incumbent.
4. Staffing plan with transition team members identified by name, position, start date, and responsibilities.
5. Risks to the transition effort and risk mitigation and transition contingency plans in the event the transition cannot be executed on schedule.
6. Method of communication and coordination with the incumbent and the Government regarding the status of the transition, contingency actions, and schedule changes.

4.1.2 Task 2 – Program and Service Management

The Recipient must provide the management and functional support needed to manage all aspects of delivery of the SLTT SOC | ISAC services to all fifty states (plus the District of Columbia) and to as many local, tribal, and territorial government entities as possible, as appropriate for their cybersecurity maturity. The Recipient must identify a Program Manager (PM) that will provide program management activities including, but not limited to: transition planning, program/project planning, resource management, quality assurance, risk management, status and problem reporting, and administrative support.

Program Management Plan Execution

The Recipient must have submitted a Program Management Plan (PMP) as part of the cooperative agreement application Award. Upon Award, CISA PO will provide feedback on the Program Management Plan and may request revisions before any work can commence. A detailed PMP outlines how the Cooperative Agreement will be executed for CISA PO approval. The PMP must reflect, and be consistent with, the Project Budget periods and must cover the entire two years of the period of performance. The PMP must identify important objectives and deliverables and each major task or action step needed to reach those objectives and deliverables. For each major task or action step, the PMP must identify timeframes involved, including start- and end- dates. A budget and metrics will be denoted for each Major Activity. The PMP will be considered an accountable document outlining the work and expectations between the Government and Recipient regarding the full execution of the work listed in the Cooperative Agreement. Any request for work to be done from the government that the Recipient determines falls outside of this Cooperative Agreement should be identified and discussed with the government PO prior to committing any

additional resources.

Develop a Service Operational Plan

The Recipient must have submitted a draft Service Operational Plan as part of the cooperative agreement application and must make required updates throughout the Period of Performance Award to ensure information is current. Upon Award, CISA PO will provide feedback on the Service Operational Plan. The Recipient must provide a finalized Service Operational Plan within fifteen (15) working days after CISA PO comments. The Service Operational Plan will include, but is not limited to, the following:

- Service Operating Model
- Sustainability Plan
- Current Services and Activities in relation to the Service Operating Model

1. Service Operating Model

The Recipient must provide how the organization delivers value and uses multiple channels to communicate with its stakeholders. It will outline various levels of service based on the SLTT entities cybersecurity maturity model. The SLTT sector/subsectors have a diverse set of stakeholders (from small offices to large enterprise systems), with widely varying degrees of technical knowledge and cyber posture maturity. This diversity calls for the Recipient to strategically segment services, including education and outreach materials for audiences with different levels of cybersecurity knowledge and understanding. The Service Operating Model formally defines the processes needed to create and deliver value at the stakeholder's level of cybersecurity maturity. The Service Operating Model clarifies the basic structures, processes, and methods at several levels. The Service Operating Model will incorporate size-and maturity-based "target" operating models to assist SLTT stakeholders in efficiently and effectively executing on the ISAC strategy. The model must provide details of who should be given specific information, when that information should be delivered, and what communication channels will be used to convey the information. The Service Operating Model must encourage adoption of DHS cybersecurity services among SLTT governments.

2. Sustainability Plan:

The Recipient must be able to build a business model to support its activities to be sustainable in the long-term. Current organizations that are providing cyber threat information sharing services charge fees for services, as do managed service providers. The Recipient will not be expected to charge membership fees but should include a plan for sustainably providing some minimal level of threat information sharing services to the entire SLTT sector while building a plan for tiered services that would be available at additional fees to member organizations.

Staffing/Resources/Key Personnel

The Recipient must provide sufficient personnel possessing the skills, knowledge, training, and security clearances (as applicable) to perform the services required by this Cooperative Agreement.

The Recipient must ensure that its staff maintains any required professional certifications, accreditations, and proficiency relative to their areas of expertise. The Recipient must submit documentation of such records at the kick-off meeting. The staffing documentation must include the organizational structure, details on each employee's responsibilities/roles, professional certifications, and the security classification an employee needs to fulfill those responsibilities. The expenses incurred by the Recipient or by individual employees to meet professional certifications and accreditations requirements are not allowable costs under this Cooperative Agreement.

All Recipient staff must be fully proficient in the areas in which they work. All Recipient staff will routinely:

1. Maintain professional certifications.
2. Keep current with advances in relevant cybersecurity awareness and share this knowledge with other SLTT and CISA personnel.
3. Act in a consultative manner, proactively searching for creative solutions and strategies. Additionally, all recommended improvements, enhancements and/or changes to the infrastructure, tools, and cybersecurity capabilities will be shared with the CISA PO for review and approval before implementation.
4. Respond promptly, professionally, and courteously to CISA communications.
5. Freely provide knowledge transfer of work products and cybersecurity expertise associated with services.

4.1.2.1 Kick-off Meeting

The Recipient must hold a technical kickoff meeting, and present, for review and approval by CISA PO, the details of the intended transition approach, work plan, and schedule, and the plan for staffing that ensures full assumption of services. In addition, the Recipient must:

1. Specify dates, locations (can be virtual), and agenda to all attendees at least five (5) calendar days before the kick-off meeting;
2. Provide meeting minutes to the CISA attendees within three (3) business days after the meeting; and,
3. Invite, as a minimum, the CISA PO, DHS Contracting Officers Representative (COR), the DHS/CISA JCDC Associate Director, and JCDC Partnerships Chief and SLTT Staff, Strategic Operations Chief, and PMO Staff.

4.1.2.2 In-Progress Review (IPR)

The Recipient must conduct one to four Monthly In-Progress Review Meetings via teleconference with the CISA PO to provide a status report on the full range of services required under this Cooperative Agreement including, but not limited to discuss program and project status, and performance measure. The Recipient must summarize accomplishments, present analyses of major challenges, and offer innovative solutions to improve weaknesses based on established performance measures.

In addition, the Recipient must:

1. Prepare and maintain the Project Plan(s) - For each new program the Recipient must prepare a Project Plan that generally describes the technical approach, value add, output or deliverables, organizational resources involved, risk management, communication management, scope, budget, and schedule with deadline and milestones.
2. Measure, track, and evaluate progress of programs against the project plan.
3. Measure, track, and evaluate progress of a Stakeholder Publications Report on the forthcoming (e.g., 3 Months) cyber products that will be distributed to stakeholders.
4. Measure, track, and evaluate a Cyber Operations Status report. Provide status of operational support to include but, not limited to:
    - Programmatic:
        - Albert and EDR sensor onboarding and/or upgrades.
        - Number of entities using MDBR and MDBR+.
        - Health/current status of program to include cost, schedule, and scope metrics.
        - Updates on requests for information and/or support.
        - Other key programmatic metrics that may be requested.
    - Operations:
        - Top cyber-related threats to the SLTT community and related notifications and/or incident metrics.
        - Number of events and incidents reported to the ISACs (broken out weekly and a roll up for the Program Year (FY).
        - Number of incident response activities currently being conducted and a roll up for the FY.
        - Number of detections, blocks, and incidents captured by EDR sensors.
        - Number of Albert sensors deployed in SLTT CI/community (elections, education (K-12), water).
        - Other key operational service metrics that may be requested.

The Recipient must provide the CISA PO with agenda and materials that will be discussed during the meeting at least three (3) business days before the

meeting. The Recipient must publish the action items from each IPR by the close of business the following day.

4.1.2.3 Program Management Review (PMR)

The Recipient must conduct quarterly strategic review meetings via teleconference with the CISA PO and CISA Leadership team to monitor progress of the program and its technology implementation from a strategic level and make sure that objectives are on track. Quarterly meetings will focus on where enhancements and efficiencies may be attained, the problems that are occurring in the implementation, why they are happening, what strategic actions will correct them, and who will have responsibility for achieving the targets.

In addition, the Recipient must:

1. Work with the CISA PO to institute a process of collecting and reviewing information to help make long-range strategic decisions on a quarterly basis.
2. Define its program and technology strategy, or direction of programs.
3. Measure, track, and evaluate progress against a Stakeholder Engagement Report.
    a. The Recipient must provide the CISA PO a list of all forthcoming (e.g., 3 Months) conferences, meetings, and other travel engagements. At a minimum, the list must define the following for each event: title, host organization, date(s), name of employees, role of employee at event (e.g., speaking), POC at travel location, task that the travel supports, purpose, and listing of expenses planned.
4. Recipient executive leadership must present a review of the strategy map/plan, offering perspectives on the programs it must prioritize.
5. Ensure that upgrades, improvements, and program services move towards an agreed-upon end.
6. Ensure that quarterly meetings incorporate review and decisions on allocating resources to pursue this strategy. They may also extend to control mechanisms for guiding the implementation of the strategy.
7. Develop a health plan for each program with clear thresholds.
8. Provide materials to the PO at least three (3) business days before each PMR.
9. Provide meeting minutes to the PO within two (2) business days after the meeting.

4.1.2.4 Ad Hoc Reporting

Within the fifteen (15) days after Award, the CISA PO and the Recipient will design and agree on a standard reporting format for Monthly Status Reports to include the following information at a minimum:

1. Programs during reporting period, by task (Include: On-going programs, new activities, completed activities, progress to date on all activities). Start

each section with a brief description of the program.
2. Schedule (Shows major tasks, milestones, and deliverables, planned and actual start and completion dates for each).
3. Monthly Performance measures and metrics to include those defined in Task 10.
4. Problems, down-time, and corrective actions taken.
5. SLTT stakeholder needs, issues or concerns and proposed resolutions to address them.
6. Financial Status Report delineated by fixed/variable cost drivers that define logical elements of capability. Report will include, but not limited to: Funding burn rates (Monthly) - Budget, Forecast, Estimate At Completion (EAC), Budget vs EAC variance.
7. Earned Value Management (EVM) statistics.
8. Comparison data / cost sharing model between states and the Federal Government.
9. Personnel gains, losses, and status (security clearance, etc.).
10. Issues or key risks, including constraints (e.g., cost, schedule, etc.,) and assumptions, and planned responses for each.
11. Challenges and Government actions required.

For special Proofs of Value, the Recipient must provide a report on the successful accomplishment of major milestones/deliverables within the planned project schedule and costs. Project reporting must also address any issues, problems, risks, or concerns that could negatively impact the project.

Per the Terms and Conditions, the Recipient must provide CISA with the report by the date requested by CISA PO and include a statement regarding the Recipient's approach to implementing the BOD or ED (e.g., the BOD or ED has been implemented, or a compensating control or other mitigation is in place.)

The Recipient must provide the CISA PO a monthly list of all planned conferences, meetings, and other travel engagements. At a minimum, the list must define the following for each event: title, host organization, date(s), name of employees, role of employee at event (e.g., speaking), POC at travel location, task that the travel supports, purpose, and listing of expenses planned.

The Recipient must provide CISA PO with a Trip Report monthly for all travel that is completed. The Recipient must identify the travel, to include: the name of the employee, location of travel, duration of trip, POC at travel location, task that the travel supports, benefit to the scope of work, accomplishments/lessons learned, and itemized listing of expenses.

4.1.2.5 Meetings

The Recipient must support recurring status meetings and conferences by preparing and delivering Meeting Agendas, Meeting Minutes, Presentation Materials, and an Action Item List for the meeting and/or conference.

The following instructions are applicable to all federal meetings and/or conferences:

a. The Recipient must propose a date/purpose for a meeting and/or conference for the CISA PO's approval.

b. For all presentations, CISA PO reserves the right to revise the agenda and/or presentation materials. The Recipient must provide appropriate personnel available to respond to CISA questions. The Recipient must prepare and deliver presentation materials three (3) business days prior to the start of each scheduled conference, meeting, and/or review.

c. The Recipient must record and submit minutes. The Recipient must track action items. Each assigned action item will have a due date and responsible CISA PO or Recipient person(s) assigned, who will provide the status of the action at agreed upon intervals until the action is closed. In the event an action item cannot be closed promptly, a plan of action will be developed for closure.

4.1.3 Program Management Deliverables

The Recipient must provide the deliverables listed in the following table:

Deliverable	Due Date	Type
Program Management Plan	Draft: At Award Final: Fifteen (15) business Days after Government Comments Minimum of Semi-annually; update as needed	Formal
Service Operational Plan	Draft: At Award Final: Fifteen (15) business Days after Government comments	Formal
Staffing Plan	Draft: At Kickoff Meeting Final: Fifteen (15) business Days after Government Comments; update as needed	Formal
In-Progress Review (IPR)	Three Business days prior to scheduled IPR One to Four IPRs per month	Formal

Deliverable	Due Date	Type
Program Management Review (PMR)	Provide PMR slides three business days prior to PMR. Meetings are held quarterly.	Formal
Meeting Agenda, Minutes, Action Items	Agenda: Five (5) business days prior to meeting Minutes and Action Items: Two (2) business days after meetings	Formal
Implementation of Binding Operational Directives (BOD) and Emergency Directives (ED) Report	30 days after Award	Formal
Project Plan	In the event of an agreed upon new program: Required no later than 15 days prior to work commencing	Formal

4.2 Functional Area 2: Cybersecurity Operations Center Services

4.2.1 Task 3- Threat Monitoring and Analysis

Monitoring and analysis must consist of security event detection, categorization, prioritization, and collaborative reporting. The Recipient must:

1. Provide the monitoring and analysis services described in this scope of work.

2. Provide 24x7x365 Security Operations Center (SOC) for real-time cybersecurity event monitoring, synthesizing, and analyzing threats directed at the SLTT sector and its critical infrastructure sub-sectors (e.g., Elections).
    - Maintain a team of highly trained and experienced cybersecurity personnel; SOC staff maintains cyber-security certifications and use state-of-the art tools to escalate intrusion events/incidents at near-real time speeds.
    - Monitor threat data and determine where possible security events must be investigated.
    - Investigate and positively review anomalous alerts that are detected by security devices or reported to the SOC from external entities, CISA, and/or the SLTT community to include but not limited to, via collaboration platforms, incoming phone calls, emails, workflow ticketing and SOC tools.
    - Create a sector level view of threat activity through demonstrated

utility of a general Cyber Threat Framework (CTF). Take defensive artifacts like behavioral analytics, intel on adversary behaviors or vulnerabilities across the sector/subsectors and map them to a threat modeling framework technique.

3. Maintain situational awareness of current threat activity and risks by mining open-source and classified data sources and coordinating with cyber experts, government, and private sector Cyber Threat Information and Incident Response capabilities, other ISACs, SLTT fusion centers, law enforcement agencies, counterintelligence analysts, and representatives from CISA and partner Federal government agencies.
4. Identify trends in security threats and their potential impact on the SLTT community and sub- sectors.
5. Develop and maintain appropriate countermeasures for protection, defense, and response.

Cyber Analysts/Liaisons to CISA

CISA provides an organization for cyber analysts from the ISAC to liaise with CISA operations. The Recipient must provide an adequate number of liaisons with a Top Secret / SCI clearance to act as cybersecurity analysts and perform the following analytic and liaison functions. The minimum number of liaisons is eight and CISA will work with the Recipient if additional liaisons are needed.

1. Monitor and analyze security issues. Provide 12x5 staffing and after hours on-call cyber analysts to analyze and evaluate the rapidly changing threat landscape and sophisticated threats to SLTT sector.
2. Research threats. Consolidate and conduct comprehensive analysis of threat data obtained from classified, proprietary, and open sources to develop improved information on cyber threats against SLTT unclassified networks.
3. When requested by CISA, conduct cyber threat analysis of malicious activity that is or has the potential to impact SLTT networks and provide detailed analysis of potential patterns, proposed next steps, noteworthy findings, etc. Analyst will follow CISA developed Analytic Roles and Responsibilities Standard Operating Procedures. Within the scope of Recipient's technologies, analysts should be conducting the same or similar analytic processes as CISA Threat Hunting. Develop protection for tomorrow's security challenges; provide indication and warnings of impending attacks.
4. Leverage all source intelligence access to develop improved information on cyber threats and to perform advanced technical analysis on events/incidents that occur on SLTT networks and endpoints.
5. Leverage threat modeling and CTF methodologies as a resource for improving defenses in the SLTT sector and its critical subsectors (including Elections).
6. Conduct link analysis of technical data using software tools to identify trends in attacks, targeting, and timing of suspicious/malicious activity.
7. Assist the Federal Government in tracking and reporting trends on operations and intrusion incidents. Develop and actively manage network and host

intrusion detection efforts in support of current CISA priorities.

8. Deliver threat information. Produce situational, incident-related reports on cyber threats that affect SLTT networks and endpoints.
9. Produce near real-time cybersecurity alerts and advisories in support of SLTTs' network defense and cyber resiliency. Provide CISA a weekly summary of anticipated and planned ISAC developed products for dissemination to include but not limited to, white papers, advisories, alerts, and reports. Where possible, support and co-seal CISA-led network defense alerts and advisory products. Respond to information requests as required and perform specialized cyber threat analyses and reports for external organizations/partners, upon approval from the CISA PO and CISA Operations Manager.
10. Respond to information requests from Threat Hunting Mission Coordinators or designees.
11. Conduct cyber threat analysis on intelligence shared from Mission Teams for potential impacts to the SLTT community
12. Query Albert with unique IOCs provided by Mission Coordinators and provide results, analysis and proposed next steps for consideration.
13. Perform advanced analyses of potentially malicious activities that have occurred or are believed to have occurred on SLTT networks and endpoints.
14. At CISA's request, prepare and provide threat briefings on SLTT cyber landscape.
15. Contribute to working groups, task forces, exercises, and committees and provide relevant information in support of SLTT objectives.
16. Within the scope of their technologies, ISAC analysts will follow the same or similar analytical processes as CISA Threat Hunting, as required.
17. At CISA's request, record certain information related to this task in CISA's incident ticketing system.

Deliverable includes:

Deliverable	Due Date	Type
Anticipated and Planned Products for Dissemination	Weekly	Formal

4.2.1.1 Identify and Prioritize Assets

Identification and prioritization of assets is an important piece of understanding the services offered to SLTTs. The Recipient must:

- Identify what cyber-connected assets – to include data, devices, systems, and operational technology, which control systems designed to operate physical processes – are most critical for the SLTT community and subsectors (including Elections) to fulfill their primary objectives.
- Maintain SLTT Network infrastructure information to include Domain, IP ranges, and IPs of critical assets.

- Implement workflow with CISA to maintain SLTT customer management information in a format sharable for Federal Government network defense initiatives.
- Define methodology for how critical asset information will be used via rules for monitoring technology.

4.2.1.2 Threat Triage, Impact Analysis, Research

In order to establish an understanding and plan to mitigate cyber threats, the Recipient must:

- understand trends in threats, vulnerabilities, interdependencies, and potential consequences over time to provide investigative and response activities for the SLTT and Elections Communities;
- enable awareness around cybersecurity threats with the aid of technology, using multi-tenant event monitoring and analysis; and,
- establish a centralized location for the SLTT/Elections cybersecurity communities to collect and analyze evidence of malicious activity that is relevant to the sectors and manage indicators that enhance defensive actions and improve resilience.

The SOC analyst must:

- drive bi-directional cyber threat sharing between SLTT/Election community members and the SOC analyst team via a multi-tenant Threat Intelligence Platform (TIP); and,
- generate context for quickly identifying and remediating threats. Analysts gather data points, document indicators, and add context to indicators within the TIP. Context may include but is not limited to: Traffic Light Protocol (TLP) ratings, target areas, intent/campaign attribution details, tactics, techniques, and procedures (TTP), and links to related references to support real-time decision making. The TIP must be accessible to the SLTT/Elections trusted member circle (including CISA SLTT Cybersecurity Analysts) to consume, share evidence and discoveries, exchange information, and ensure similar threats are addressed in a repeatable, efficient manner.

SOC staff must constantly keep up with the latest threat information, monitor darknet chatter, and leverage threat information to feed cybersecurity tools to improve SLTT detection, analysis, and prioritization mechanisms.

4.2.1.3 Security Event Impact Classification and Prioritization

The Recipient must provide comprehensive real time cybersecurity information about the SLTT sector and sub-sector (e.g., Elections) threat landscape in order to apprise SLTT cyber coordinators and stakeholders about the cyber “big picture” that is relevant to SLTT organizations. To provide effective warnings, threats must be narrowed to those that could have the most consequential impact to the assets identified in step 4.2.1.1. The Recipient must:

- Provide human-in-the-loop event analysis and provide post-analysis categorization, prioritization, and recommendation of event disposition.
- Teams filter IP/URL data into specific threat categories.
- Analysts access and analyze data, and collaborate, research, comment, organize, and support an active cyber scoring process for indicators of compromise in near real-time.
- Maintain traceability between evidence, indicators, rules, and sensors to identify why a rule is created and the type of activity it detects.
- Rank and categorize events and incidents based on the incident severity, impact, and agreed upon thresholds.
- Respond to CISA request for information on events and incidents within a reasonable time.
- Communicate scoring of events and incidents to CISA.

4.2.1.4 Security Event Pattern/Rule Design

Identifying security event patterns and rule design are a key part of assisting the SLTT/Elections community. To fulfill this task, the Recipient must:

1. Determine indicators, including command and control channels, for malicious code.
2. Provide recommendations specific to tactical internet filtering or other measures to mitigate cyber threats.
3. Develop, implement, and disseminate new security content, such as IDS rules (signatures) and cyber threat indicators, based on cyber threat information and the results of the SOC's own analysis.
4. Produce relevant, high-quality indicators to be shared into the TIP/Automated Indicator Sharing (AIS) tool for distribution to the SLTT/Elections sectors and Federal Government.
5. Perform analysis of SLTT/Elections community-collected traffic against classified cyber threat indicators
    - CISA will be responsible for:
        - Sharing unclassified and classified Government Furnished Information (GFI) up to Top Secret/Sensitive Compartmented Information (TS/SCI);
    - ISAC will be responsible for:
        - Maintaining a certified Sensitive Compartmented Information Facility (SCIF) to process classified information and facilitate collaboration with Federal cyber centers.
        - Providing CISA access to the analysis performed with classified indicators in order to generate ad hoc reports.
        - Coordinating with CISA, in the event of a suspected true-positive match.
        - Providing sensor log/netflow data for further analysis to detect possible intrusions into SLTT/Elections networks.

- Maintaining a Personally Identifiable Information (PII) review process prior to sharing data in accordance with CISA (Cybersecurity Information Sharing Act) and the DHS operational guidance.

6. Provide IDS Signature Management. The Recipient must:
    - Identify a process for generating signatures that shall be incorporated into Albert IDS.
    - Maintain 24x7x365 operational availability to build, test, and deploy customized Intrusion Detection System (IDS) signatures.
    - Track the lifecycle of Federal government indicators to include types of malware, frequency of alerting, vulnerability trending/timeline, signature classifications, etc.
    - Develop, test, and deploy customized signatures based on specific sets of indicators shared by CISA within one business day of the data transfer/receipt of the indicators.
    - Report Event/Incident Analysis and/or improvements (e.g., overcome false positives) in the Daily Report to CISA.
    - Conduct joint analysis with CISA analysts to correlate signatures enabled in Albert and in Einstein. Tune systems periodically to share commercial signatures and synchronize signature detection for similar activity across SLTT/Elections and Federal networks.

4.2.1.5 Security Event Notification

Security Event Notifications are the product of security event analysis but may be generated based on information from other sources, such as intelligence reports, incident reports from Component SLTTs, etc. Notifications are the primary means for the ISAC to coordinate with Component SLTTs/Elections entities regarding security event analysis and are sent whenever the ISAC becomes aware of activity that may pose component SLTT/Elections security risks.

The Recipient must:

- Provide notifications to SLTT/Elections Components in a timely manner as indicated in a current Security Event Notification SOP.
- Escalate security event reports as defined in membership agreements, to initiate containment activities.
- Maintain an up-to-date list of Department, SLTT/Elections Component, and relevant entity points of contact.
- Report daily notifications and status updates to the CISA PO and Operational Leads.
- Manage the resolution of security events that affect SLTT/Elections information systems using an event ticketing system.
- Recipient must have structured sector distro and contact lists for SLTT communities, including but not limited to: K-12, water, health, and public health. Sector distro lists will be utilized to ensure network defense

information, sector specific messaging, and/or cyber activity alerts are directly distributed to those who have a need to know.

4.2.2 Task 4 – Incident Assessment and Management

To actively participate in identification, analysis, and incident response activities in support of any reported SLTT and/or Elections cybersecurity event or incident and in coordination with CISA and other partner organizations, the Recipient must:

1. Serve as a central point of contact and communications for all unclassified SLTT/Elections computer- related security incidents.
2. With CISA's review and approval, develop a repeatable threshold mechanism to evaluate and score the severity of cyber incidents and potential impacts to SLTTs/elections.
3. After analysis is conducted, security events may be classified as security incidents.
4. Classify the severity of security incidents in accordance with the National Cyber Incident Severity Schema.
5. Support reporting requirements to the Federal Government, in accordance with the NCIRP.
6. Report suspected or confirmed SLTT/Elections cyber incidents to CISA, in accordance with the ISAC and CISA CONOPS, SOPs, and process orientated documentation as applicable.
7. Coordinate and assist SLTT/Elections components in managing the cyber incident response and escalation process.
8. During incident response and recovery processes, maintain and conduct status updates with affected entity, develop reports as needed, update associated tickets, disseminate CIRT Daily Ticket report to appropriate CISA Recipients, and other tasks as necessary.
9. Actively engage the SLTT/Elections entity to share and coordinate CISA Threat Hunting services, including when the affected SLTT/Elections entity may be interested in Federal government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.
10. Follow the Vulnerability and Incident Coordination Process SOP.

Deliverable includes:

Deliverable	Due Date	Type
Threshold Mechanism for Severity	Annually	Formal

4.2.2.1 Cybersecurity Incident Response Support

The ISAC provides technical expertise to manage, coordinate response and

remediation communications, document, and report on computer security incidents.

The Recipient must:

1. Provide 24x7x365 incident response management and support.
2. Coordinate with SLTT/Elections Component SOCs on planning and executing cybersecurity incident remediation actions.
3. Conduct research on threats, assess the situation, determine relevance to the SLTT/Elections environment, provide security situational awareness, and coordinate with CISA Threat Hunting Leads as necessary.
4. Disseminate relevant security event data, cyber threat information, and other cybersecurity related information to the SLTT/Elections Community.
5. Coordinate and advise on incident response actions conducted by SLTT/Elections entities SOCs for incidents affecting their environments.
6. Assist in conducting and coordinating victim notifications to SLTT/Elections entities in accordance with CISA's notification processes. Provide notification details to CISA upon request.
7. Assist security investigations by applying asset criticality, identity, vulnerability information, and the location of sensitive digital assets.
8. Assist with incident control and containment.
9. Interview individuals involved in a computer security incident.
10. Collect any information (logs, PCAP, hard-drive, forensic image, etc.) that will be used for analysis.
11. Collect, document, maintain chain-of-custody rules, and preserve computer security incident response evidence.
12. Perform forensics investigations to identify incident root cause or source, extent of damage, and recommended countermeasures.
13. Prepare reports describing incident investigations.
14. Make recommendations to prevent, disrupt, reduce, bypass, and correct conditions of possible future similar incidents.
15. Provide remediation and mitigation guidance as a result of cybersecurity incidents.
16. Utilize an incident tracking system to track the incident from cradle to grave.
17. Develop thresholds, in coordination and agreement with CISA, for necessary onsite incident response activities.
18. Conduct virtual incident response activities with SLTT/election entities when necessary.
19. Apply expertise to assess damage, mitigate, and recover from an incident.
20. Escalate cyber response activities in accordance with Incident Management CONOPs, SOPs, and playbooks, as applicable.
21. Extract all high severity and high confidence Indicators of Compromise from analysis and automatically ingest into the threat intelligence platform for indicator scoring, and based on criticality, use them to create signatures for deployment in Albert and for sharing with CISA.
22. Collaborate and share incident response details – IOCs, threat actor TTPs, etc. – with CISA components during incident response engagements.
23. Coordinate with CISA components, including regional staff, to provide remediation and mitigation guidance to SLTT/Election entities.

4.2.2.2 *Incident Analysis*

The Recipient must analyze all the artifacts from an SLTT/Elections intrusion to establish a timeline, determine the origin of the intrusion, identify what actions were taken to make the intrusion successful, determine the motivation (what the actor was after), develop a mitigation plan, and support recovery steps from the incident. In addition, they must:

- Document suspected incidents as required to support law enforcement records, case disposition, and audit reviews.
- Provide a forensic report to CISA components to include the following details: incident severity, potential or experienced impacts, assets targeted, success of threat actor, adversary motivation (if possible), recommendations for mitigation and remediation, and next steps.
- Lessons Learned must be documented after every major incident, and the Recipient provide these through recommendations to relevant SLTT/Elections via incident reports and lessons learned calls following an incident. Examples of major incidents include, but are not limited to those that present:
    - An imminent threat to life or safety
    - An imminent threat to critical infrastructure
    - Evidence of coordinated and/or nation-state sponsored cyberattack activity against SLTT/Elections
    - Widespread active exploitation of numerous SLTT/Elections organizations
    - Other features that the Recipient or CISA leadership determine rise to the level of a major incident

Deliverable includes:

Deliverable	Due Date	Type
Forensic Report	Within 1 week of closing out incident analysis	Formal

4.2.2.3 *Counter Measure Coordination*

The Recipient must work with appropriate organizations to define and disseminate mitigation and recovery actions.

4.2.3 Task 5 - SLTT Cybersecurity Situational Awareness

To ensure there is a complete, current view of the SLTT cybersecurity landscape, the Recipient must:

- Produce a 24x7x365 globalized view of the ever-evolving cybersecurity threat landscape for the SLTT sector and its critical infrastructure sub-sectors (to

include at minimum the Elections sub-sector).

- Maintain an SLTT (and critical subsectors, at minimum **Elections**) National Alert Level Map with time sensitive updates on Homeland Security Information Network (HSIN), as well as the Situational Alert Map, to reflect cyber incident notifications and status of threat level and incidents.
- Equip SLTT/Elections cyber coordinators with a 24x7x365 threat intelligence sharing platform that enables users to rapidly research the latest security threats, aggregate actionable information, and provide a foundation for analysis and decision-making. Decisions shall be based on information collected from collaborative analytic peers from the stakeholder community, which facilitates data exchange of **cyber threat activity** for generating actionable and relevant threat feeds for consumption by cyber defense products/systems.

4.2.4 Task 6 - Malware and Forensic Analysis

Upon the transition to Malware NextGen, the Recipient must support the operation of Malware NextGen by verifying that SLTT entities seeking to participate in Malware NextGen are members of the ISAC funded by this Award. In doing so, the Recipient must integrate its information systems with CISA's in order to facilitate this verification process. The Recipient must continue to perform the following functions until the transition to Malware NextGen as operated by CISA is completed:

- Maintain a Malicious Code Analysis Platform (MCAP), a fully automated service that enables members to submit suspicious files or URLs for analysis in a controlled and non- public environment via an easy-to-use front-end portal. This will enable:
    (1) reporting technical or behavioral indicator details and actions that were observed during malware execution;
    (2) analysis that helps guide incident remediation in a timely manner;
    (3) situational awareness regarding potential trends in malware; and,
    (4) ability to ingest near real-time indicator data into the threat intelligence platform and perform scoring operations.
- Provide 24x7x365 support for advanced network and digital media forensic analysis activities, malicious code reverse engineering and analysis to assess the malware threat characteristics and determine the root cause of an incident on a system. Activities include:
    - Ensure that personnel are appropriately trained and certified in forensic analysis processes and the specific tools selected.
    - Adhere to policies and procedures for preserving chain of custody of equipment as part of investigations, as required.
    - Implementation, training, SOP development and maintenance of implemented solutions.
    - Perform offline analysis in an isolated lab environment.
    - Hard drive (and other storage device) analysis of suspected

systems impacted by malicious activity, to include occasional hard drive imaging.
    - Advanced code analysis of detected malicious code.
    - In-depth log file analysis to determine trend, patterns, and suspicious activity.
    - Pattern analysis, trend analysis, behavior analysis and other specialized analysis.
    - Extract high severity and high confidence indicators of compromise (IOCs) from forensic analysis.
    - Provide remedial recommendations and produce consistent comprehensive reports on findings.
- Provide automated SLTT case data reporting with CISA and indicators into the Threat Intelligence sharing platform for awareness on a national level.
- IOCs will be ingested into the threat intelligence platform for indicator scoring and based on critically may be used to create signatures for deployment in Albert.
- Transition all or parts of this service to CISA based on an agreed upon transition project plan and milestones.

4.2.5 Task 7 – Vulnerability Management Analysis

A key competency of the SOC is its ability to focus on technical vulnerabilities in commercially available hardware, firmware, and software products used by the SLTT/Elections community. SLTT/Elections components are responsible for correcting site-specific vulnerabilities; however, the ISAC SOC will assess vulnerabilities to the SLTT/Elections.

The Recipient shall:

1. Monitor new and known vulnerabilities, threats, and applicable patches, hotfixes, and firmware upgrades, which have the potential to impact the SLTT/Elections risk posture and assess their risk to the cyber infrastructure and applications.
2. Provide timely information security alerts, advisories, and bulletins following an established notification program.

4.2.5.1 SLTT Vulnerability Landscape

To enable understanding the vulnerability landscape, the Recipient shall:

1. Share awareness of free CISA services including, not limited to, Cyber Hygiene vulnerability scanning and web application scanning with the SLTT/Elections community.
2. Assess data from many sources to provide a contextualized view of the vulnerability risk to the SLTT and its critical sub-sectors (e.g., elections, etc.) and share summarized data of prevalent and exploited vulnerability trends to CISA.

3. In coordination with CISA, track SLTT/Elections-wide component timely response to critical alerts, advisories, and bulletins.
4. Perform vulnerability trend analysis to compile long-term recommendations and reports for security areas of interest.

4.2.6 Task 8– Coordinated Vulnerability Disclosure Program for SLTT Election Offices

To fulfill SLTT Election offices' needs in regard to the coordinated vulnerability disclosure program the Recipient shall:

1. Maintain a formalized process to receive, validate, and transmit elections environment vulnerability information from security researchers and other qualified sources to the appropriate election office or vendor Coordinated Vulnerability Disclosure (CVD) Program.
2. Maintain Guidelines and Policy for the Program in Coordination with Elections Infrastructure Subsector Government Coordinating Council (GCC), Sector Coordinating Council (SCC) and the Sector Risk Management Agency (SRMA).
3. Maintain infrastructure for submitting/ingesting discovered vulnerabilities and making notification to participating election entities.
4. Elicit CVD participation from state and local election entities and security researchers/vendors.
5. Publicize CVD election entity participants (and vendors, if desired) alongside program guidelines/policies.

4.2.7 Task 9 – Threat Reporting

The purpose of this activity is to share tactical cybersecurity information across the SLTT and its subsectors to pre-emptively stop threats by providing mitigation actions. Through information sharing, the ISACs provide strategies to reduce cyber risk. Members are provided a means for customized alerting and reporting that is accessible via a collaborative portal (i.e., Threat Intelligence Platform). Reporting products follow a standardized labeling format with criticality of the report as part of the subject line.

Recipient shall assist the Federal Government with dissemination of cyber threat information to SLTT/Elections cybersecurity coordinators and Computer Network Defense communities (e.g.
Component SOCs, SLTT Cyber/Fusion Centers, critical infrastructure, and sub-sector communities, etc.). Much of the information created by the ISACs will be specific to particular types of cyber threats, but CISA may elect to publish more generalizable education materials funded through other CISA-sponsored publications, websites, or with other CISA Recipients. CISA may share particular cyber threat information if it is necessary to publicize particular threats more broadly.

SLTT and its critical subsector community is provided with daily, weekly, and monthly SLTT/Elections Cyber Reporting. The Recipient shall at minimum:

1. Analyze and report on unique attack vectors, emerging cyber threats, new vulnerabilities, and current trends used by malicious actors.
2. Share and distribute any and all Tactics, Techniques, and Procedures (TTP) to SLTT/Elections that would help SLTT/Elections identify and thwart or protect themselves from an attack or intrusion.
3. Prepare briefing materials, provide cybersecurity thought leadership and best practices, and conduct threat briefings.
4. Provide threat reporting in machine-readable form, where possible and appropriate to do so. Machine-readable formats will allow consumption across the widest stakeholder community security tools for automated network defense.
5. Communicate current and evolving threat report distribution capabilities/methods, including machine-readable methods to members to ensure members are aware of security tools integrations.
6. Gather feedback from members' preferred threat reporting methods, and document barriers to more advanced reporting capabilities, such as automated machine-readable feeds.

4.2.7.1 Alerts/Advisories

The Recipient shall advise SLTT and subsector members on critical cyber incidents, vulnerabilities, and threat information. These alerts provide:

- Timely, relevant, and actionable information for cyber coordination issues that arise.
- Criticality of the Alert (part of the standardized product subject line labeling).
- Anonymization to protect the source of the information.

4.2.7.2 Daily Status Report

The Recipient must provide CIRT Ticket Reports Daily to CISA Threat Hunting and JCDC and join at least two weekly meetings with JCDC to discuss administrative and operational focus areas. In addition, they must:

- Provide daily reports to the CISA PO, Officer, and SLTT/Elections Operations analysts detailing all escalated security events, incidents responded to, and priority watch list activity.
- Submit reports according to the procedures and reporting established in CONOPs. Daily operating status information includes but is not limited to:
    - Security Incidents and Event Notifications detected or reported within the past 24 hours
        - The following minimum information shall be

included in status reports: SLTT/Elections component, Functional Impact, Information Impact, Timestamp First Detected, Location of observed activity/sensor, and TTP Analysis.

- Intrusion detection signatures
    - Activity related to CISA Priority Intelligence Requirements (PIRs) will be prioritized and highlighted.
- Security device outages
- Vulnerability advisements
- Threat alerts released in the previous 24 hours

4.2.7.3 Weekly Status Reports

The Recipient must deliver to the SLTT entity (and its critical infrastructure sub-sectors; at minimum- elections) an analytic summary, tailored to each sensor monitored, outlining observed hit activity, threat trending and metrics analysis conducted on a weekly basis, in addition to Malicious Domain Blocking and Reporting (MDBR) reports weekly to SLTT members.

4.2.7.4 Monthly Reports

The Recipient must deliver a cumulative Situational Awareness Monthly Report on the SLTT/Elections threat landscape and its critical infrastructure sub-sectors (at minimum- elections) within five (5) days following the end of each month that includes but is not limited to:

1. Top Threats.
2. Top Methods.
3. Top Actors.
4. Number of incidents broken out by type.
5. Incident trending by type.
6. Major incident summaries and responses.
7. Percentage of incidents mitigated through the captured indicators in relation to outside notifications or other means.
8. Number of indicators created.
9. Tool performance/use – This will be a measure of tool performance, primarily to identify the effectiveness of tools for comparison and other metrics.

4.2.7.5 Ad Hoc Reports

The Recipient must provide ad hoc reporting, as requested. For example, the Recipient might perform complex scripting with the ability to output the results in a

variety of formats (to include HTML, XML, or other type most appropriate for the task) to repurpose the results for reports targeting different technical levels (e.g., analysts, management, etc.).

Through CISA's substantial involvement in the scope of work, it may request the Recipient deliver a Status Report providing the cybersecurity posture and threat landscape for the SLTT/Elections community. The status report must include but is not limited to:

- SLTT/Elections Top Threats, Top Methods, and Incident summaries
- Sharing best practices, network defense, or intelligence products under development

4.2.7.6 Standard Operating Procedures (SOPs)

For standardization of operating procedures and to ensure steady-state and operational functions, the Recipient must:

1. Develop and maintain formal, documented SOPs that are delivered for the CISA PO's review and approval when developed or modified.
2. Review and update all Standard Operating Procedures quarterly.
3. Maintain documentation within a shared central repository for oversight by CISA PO.
4. Provide SOPs that include the operational basis for the CISA CONOPS, CISA to SLTT/Elections communications, and any Memoranda of Agreement (MOA) between SLTT/Elections and CISA.
5. Develop end-to-end (E2E) SOP documentation that defines the current state of functions and process methodology for steady state information sharing processes between CISA, its federal cyber partners, and the SLTT/Elections stakeholder community.

   SOP Documentation includes but is not limited to:

   - Mission, function, operating rules, and charter for the ISAC
   - Code of Conduct
   - Handling and safeguarding all GFI and derivative information in accordance with all DHS security guidelines
   - Handling and safeguarding Secure Management Network (SMN) equipment in accordance with all DHS security guidelines
   - Service Level Agreements
   - Vulnerability Management and Process Integration
   - Threat Intelligence & Analysis Process Integration
   - Risk Management & Assessment Process
   - Mitigation Process (including signature development)
   - Event Notification
   - Incident Management
     - Incident Escalation

    - Victim Notification
    - Incident Response Coordination
    - Incident Communications Plan
- Reporting
- Information Sharing

4.2.8 Task 10 – Performance Measures and Metrics

The Recipient must work with the DHS/CISA Program Officer to develop, refine, deploy, and execute Performance Metrics for the Cooperative Agreement, with all proposed measures approved by the DHS/CISA Program Manager before commencement of data collection. All Performance Objectives are based on a 2-year Period of Performance. Upon Award, DHS/CISA and the Recipient will jointly develop metrics for those programs that do not have them. Should the Recipient meet a Performance Objective, the Recipient and DHS/CISA PO will work together to define a new Performance Objective.

The Performance and Metrics for this Cooperative Agreement must include but are not limited to:

- Trending Analysis and growth rate of SLTT/Elections Membership
- Utilization and rate of cyber threat exchange by the SLTT/Elections community on threat modeling and automated bi-directional sharing across the threat intelligence sharing platform
- Enhancing the degree and effectiveness of threat detection across the SLTT/Elections infrastructure through validation of indicator relevancy
- Qualitative and quantitative measures and metrics on the impact of SLTT cybersecurity incidents. The Recipient must characterize information losses during each significant SLTT/Elections cybersecurity incident and estimate remediation costs associated with the incident
- Analysis of cybersecurity events, incidents, and incident response metrics and trends, with the goal of anticipating emerging and evolving threats, and implementing countermeasures and mitigations that disrupt a wide range of attacks

The metrics must comply with the Federal Integrated Business Framework (FIBF) model for Security Operations Centers (https://ussm.gsa.gov/fibf-cyb-soc/). This ensures that any SOC-related services/solutions the ISACs deploy align with federal baseline business standards that can serve as a common understanding of what services agencies need and solutions they should offer.

Table 1 provides key performance parameters for measuring effectiveness of information sharing, analysis, and response during the Period of Performance. Measures will be recorded based on the overall SLTT/Elections community as well as segmented by CI sub-sector (i.e., Elections at minimum). Objectives stated are for a full performance year.

Performance Measure/Metric	Performance Objective
Membership	
ISAC	
Total Membership	17,000
New Members	2,000
Average Monthly Growth Rate	2% (YOY)
State Members	50
Local Government Members	20,000
Tribal Members	40
Territorial Members	6
Fusion Members	80
CI/Community	
Associations/Authorities/Commissions/Councils of Government	Count
Aviation/Port Authority	Count
Electric Utilities	Count
Elections Infrastructure	Count
Emergency Management Services/Fire/Law Enforcement	Count
Fusion Centers/Intrastate/Interstate/Regional Entities	Count
Guard	Count
Health	Count
Higher Education	Count
Judicial	Count
K-12	Count
Legislature	Count
Libraries	Count
Maritime/Port Authority	Count
Transportation	Count
Water/Wastewater Treatment	Count
Elections Infrastructure ISAC	
Total Membership	3,900
New Members	400
Average Monthly Growth Rate	0.50%
State Government Members	50
Local Government Members	3,900
Territorial Members	6
Supporting Members	50
Threat Intelligence Platform (TIP)	
Members Consuming Threat Intelligence Services	4,750
Number of ISAC Members with Analyst1 Access	50
Number of Elections Infrastructure ISAC Members with Analyst1 Access	50
Static Lists Members	4000
MISP Members	20
Cyware STIX/TAXII Real-time Feed Members	500
Number of IOCs added for static lists	Count
Number of IOCs or TTPs added for MISP	Count
Number of IOCs added from SOC Workflow	Count

Performance Measure/Metric	Performance Objective
Indicators Deprecated	Count
Number of TTPs added from SOC Workflow	Count
Known False Positive Rate on ISAC Customized Signatures	Count
Netflow Volume (PB)	Count
Stakeholder entities that provided threat intelligence (manually processed)	Count
Stakeholder entities that provided threat intelligence (directly into TIP)	Count
Stakeholder entities that provided threat intelligence (via Cyware)	Count
Total Stakeholder entities who provided threat intelligence	Count
Number of Technical Engagements to enable member use of automated threat intelligence	Count
Number of new threat groups tracked	Count
Number of new campaigns tracked	Count
Feed efficacy (indicators added, expired, uniqueness)	Count
Total number of 3rd party feeds/information sources ingested	Count
Number of campaign/threat groups directly targeting SLTT	Count
Indicators Enhanced with Intelligence	Increased rate compared to normal rate
Outreach	
HSIN Accounts - ISAC	Count
HSIN Accounts - Elections Infrastructure ISAC	Count
Member Engagement	
Regional Workshops	5
Community (e.g., State, Tribal, K-12, Public Utility, Transportation, etc.) Meetings	15
Service Reviews	250
State/Territory CISO Annual Touchpoint	60
CISA CSA Annual Touchpoint (% of CSA's contacted)	50
Total Number of Attendees at events	4,500
Event Participation	75
Situational Awareness Room Events	15
Number Days Rooms were Hosted	20
NCSR Participation - 100% Completed	5,000
Albert	
Active Albert Sensors	Count
Federally Funded Active Sensors	Count
States with an Albert Sensor(s) ISAC	Count
States with an Albert Sensor(s) Elections Infrastructure ISAC	Count
Others with an Albert Sensor(s) ISAC	Count
Others with an Albert Sensor(s) Elections	Count

Performance Measure/Metric	Performance Objective
Infrastructure ISAC	
Tribal with an Albert Sensor(s)	Count
Territories with an Albert Sensor(s) ISAC	Count
Territories with an Albert Sensor(s) Elections Infrastructure ISAC	Count
Non-Federally Funded Active Sensors	Count
States with an Albert Sensor(s)	Count
Others with an Albert Sensor(s)	Count
Tribal with an Albert Sensor(s)	Count
Territories with an Albert Sensor(s)	Count
Mean Time from Onboarding to CA Sensor Activation (days)	6 Weeks
Mean Time from Shipped to CA Sensor Activation (days)	3 Weeks
Signatures Created from AIS Indicators	
Custom Signatures developed by the ISAC (CISA/third party info)	Count
Historic Netflow Queries run in support of CISA operational activities	Count
Albert Events	Count
Albert Incidents	Count
Emergency	Count
Critical	Count
Warning	Count
Informational	Count
Mean Time from Albert Event Detection to Notification (SLA)	5 Minutes
Albert (IDS) events based on ransomware-related signatures	Count
Albert (IDS) incidents based on ransomware-related signatures	Count
Analyst Reviewed Events (Albert/EDR)	Count
CIRT	
Incidents (Differentiate by Criticality)	Count
Level 5 _ Emergency	Count
Level 4 _ Severe	Count
Level 3 _ High	Count
Level 2 _ Medium	Count
Level 1 _ Low	Count
Level 0 _ Baseline	Count
Total Number of CIRT cases opened	Count
Total Number of CIRT cases closed	Count
Local Government Members	Count
Average Resolution Time (Days) of IRTickets (Measure Received to Closed)	14 Days
MDBR	
MDBR Enrollment	6,500

Performance Measure/Metric	Performance Objective
Malicious Domain Requests Blocked (Percent of Domains Blocked Over Total DNS Requests)	<1%
Mean time from Agreement to MDBR Activation (days) (Average number of days from registration to first DNS activity)	2 Weeks
SIEM/SOAR	
Mean time to detect (abbreviated MTTD) (mins)	15 mins
Mean time to respond (MTTR) (mins)	15 mins
Number of false positives	Count
Number of events per device or host	Count
Total number of events	Count
Web Application Firewall (WAF)	
WAF Enrollment	100
Number of false positives	Count
Number of true positives	Count
CVD (VDP)	
Election Entities Participating in CVD (VDP) Program	10
Researchers/Vendors Participating in CVD (VDP) Program	Count
Vulnerabilities Reported	
Vulnerabilities Validated	
Vulnerabilities Remediated	
EDR	
Approved Endpoints Covered by EDR	50,000
EDR Entities (CA-only)	250
EDR Detections (CA-only)	Count
Ransomware Blocked by EDR (CA-only)	Count
Mean Time from Agreement to EDR Activation (days)	Count
Email Security	
Email Security Participants	100
Suppressed Email Domains	Count
Email Requests Blocked	Count
Mean Time from Agreement to Email Pilot Activation (mins)	1 min
Time to Onboard (days)	Count
Total Links Scanned	Count
Malicious Links Blocked	Count
Total Emails Scanned	Count
Malicious Emails Blocked	Count
Other Notifications	
Open Source Notifications	Count
Account Compromise	Count
CIOCC Product	Count

Performance Measure/Metric	Performance Objective
CIOCC Reported	Count
CNE Actors	Count
Compromised Server	Count
Credit Card Information	Count
DDoS	Count
Darknet	Count
Data Breach	Count
Defacement	Count
Doxing	Count
Elections	Count
Hosting Provider Takedown Request	Count
MCID	Count
Malicious Actor Activity	Count
Malware	Count
Notification	Count
Possible Botnet Infection	Count
Possible DDOS Participant	Count
Ransomware	Count
SQLi	Count
Scanning	Count
Spam/Phishing	Count
SpamHaus	Count
TLP Violation	Count
Threat	Count
Typosquatting	Count
Vulnerable System	Count
XSS	Count
Products Disseminated (Differentiate by Product Type)	
Total	Count
CIS	Count
Email	Count
Webinar	Count
Elections Infrastructure ISAC	Count
Cyber Alert	Count
Cybersecurity Spotlight	Count
Elections Infrastructure ISAC Advisories	Count
email	Count
Govt	Count
Quarterly Threat Report	Count
Newsletter	Count
Weekly News Alert	Count

Performance Measure/Metric	Performance Objective
Webinar	Count
Calendar Invite	Count
Cyber Intel Advisory	Count
Cybersecurity Advisory Summary	Count
Survey	Count
SITREP	Count
Election Security Spotlight	Count
Elections Cyber Alert	Count
Joint	Count
Email	Count
Govt	Count
Newsletter	Count
Quarterly Update	Count
Webinar	Count
Quarterly Threat Report	Count
Calendar Invite	Count
Albert Monthly Activity Report	Count
Survey	Count
ISAC	Count
Cyber Alert	Count
Cybersecurity Advisory	Count
Cybersecurity Advisory UPDATE	Count
Email	Count
Govt	Count
Quarterly Threat Report	Count
Other	Count
Newsletter	Count
SAR	Count
Cyber Intel Advisory	Count
White Paper	Count
Webinar	Count
Calendar Invite	Count
Malware Ips & Domains	Count
Global Cyber Alliance	Count
End of Support List	Count
Survey	Count
Scanning & Exploiting IPS	Count
Weekly Digest	Count
Long-Form Analytic Report	Count
Short-Form Analytic Report	Count
All ISAC	Count

The Recipient's Program Manager must meet semi-annually with the DHS/CISA PO, and CISA senior executives and their advisors. In these meetings, the Recipient's Program Manager must present a summary report describing current service trends; the availability, reliability, and effectiveness of SOC tools and infrastructure; and the Recipient's progress in continual improvement of SOC capabilities and delivery of ISAC services to the SLTT/Elections community.

The Recipient must assess the mission effectiveness and cost effectiveness of the ISAC investments in cybersecurity technology solutions. If Recipient analyses of performance and investment metrics indicate that existing operational tools may be suboptimal in capability or cost-effectiveness in protecting the SLTT/Elections community against current and emerging cybersecurity threats and attacks, the Recipient shall evaluate alternative solutions; identify, analyze, and recommend superior tools; and develop and deliver a roadmap, with funding requirements, for DHS acquisition planning.

The Recipient shall deliver the DHS Performance and Investment metrics report and briefing to the PM on a quarterly basis at the Program Management Review.

4.2.9 Task 11 – Operations Center Deliverables

The Recipient must provide the deliverables, in email format to PMO staff, listed in the following table:

Deliverable	Due Date	Type
Performance and Metrics Monthly Report	Quarterly PMR	Formal
Technology Roadmap	Semi-Annually	Formal
Standard Operating Procedures	Quarterly	Formal
SLTT/Elections Critical HVA report	Quarterly	Formal
National Alert Level Map and Situational Alert Map	24x7x365 globalized view of SLTT	Formal
Daily Operational Status Report	Daily	Formal
Liaison Officer "LNO"/SLTT Sync	Semi-Weekly	Formal

Deliverable	Due Date	Type
Managed Service (i.e., Albert) Threat Report	Weekly	Formal
Quarterly Threat Report	Quarterly	Formal
Alerts/Advisories/Notifications	Cyber relevant timeframe	Formal

4.3 Functional Area 3: SOC Architecture, Engineering, Operations and Maintenance

4.3.1 Task 12 - Security Operations Solutions

To alleviate human-centered practice that cannot keep pace with the speed and volume of current threats, the Recipient must address the paradigm of cyber defense by:

- Enabling robust cybersecurity risk management through innovation and a national SLTT/Elections shared intelligence model
- Supporting the shared intelligence model by human and machine generated information
- Integrating and automating cyber defense tasks performed by human defenders through the solution

The overarching goals are implementation independent and describe "what," rather than "how." This scope presents the minimum functionality needed for a well-conceived Security Orchestration, Automation, and Response (SOAR) service to be successful.

The Recipient must capture the overarching capabilities (an ability provided by a cybersecurity tool or product), functions (an action carried out by a cybersecurity tool or product), and activities (representing high-level processes that the Recipient undertakes to satisfy policy and governance) to enable automation of cyber defense via the sharing of cyber threat information, indicators, and intelligence. To enable these activities, the Recipient must:

1. Provide Engineering Security Operations solutions.
2. Be transparent in design and practice.
3. Create and maintain Security Operations design documentation, and security application and hardware design strategies.
4. Measure and assess cybersecurity SOC operating model maturity progress using industry best practice approaches.

Recipient shall host member wide teleconference calls as directed and when requested by CISA, to include sending invites to members, remind members of the upcoming call, encourage participation, and support meeting logistics and content.

Deliverable includes:

Deliverable	Due Date	Type
Technology Roadmap	Semi-Annually	Formal

4.3.2 Task 13 - Engineering Change Request and Security Review

To streamline and coordinate changes to program schedules, budget, or deliverables, and to ensure security compliance, the Recipient must:

1. Provide support for Change Request (CR) and security review.
2. Provide appropriate tools to enhance or replace existing tools in support of building a complete technological environment and enabling a SOC collaboration model.
3. Develop and test new applications and hardware in order to avoid obsolescence, and to improve SOC productivity.
4. Create diagrams of new or revised solutions for transition to operational support. This documentation must encompass the entire "end-to-end" configuration flow diagram describing all solution elements.
5. Devise test plans to monitor and assess the cybersecurity status of security tool components and network.
6. Provide DHS/CISA PM and Information Security Officer review of process for tracking the correction of internal self-assessment and external audit findings relating to security compliance of SOC operations and activities.

Deliverable includes:

Deliverable	Due Date	Type
Security Plan	Quarterly	Informal

4.3.3 Task 14 - Security Tool Configuration and Maintenance

The Recipient must:

1. Configure and manage SOC Platform components to include Threat Intelligence Sharing Platform (TIP), threat detection tools and devices, Security Information and Event Management (SIEM), databases, storage, and Security Orchestration, Automation and Response (SOAR) to aggregate security data and get a picture of the SLTT/Elections security landscape.
2. Perform license inventory management, license and lifecycle support, acquisition and renewal, systems analysis, hardening, troubleshooting assets, manual and automated administration/distribution, patch and update management, software update, and compliance, documentation, and utilization audits.
3. Continuously tune IDS/IPS, SIEM, SOAR, and TIP through rule/parameter creation and engineering to reduce false positives, discover previously unknown threats and increase efficiency by knowing what to work on first.

4.3.4 Task 15 - Network Defense Monitoring Architecture

The Recipient must:

1. provide advanced technical assistance to deliver a strategic architecture, and

provide engineering, design, deployment, testing, and user acceptance of network sensors in support of SLTT including Elections Infrastructure; and,

2. install, configure, and provide lifecycle maintenance/replacement of network sensor devices and managers to provision the following deliverable coverage within SLTT/Elections cloud and enterprise infrastructure.

Deliverables include:

Deliverable	Due Date	Type
1. State Infrastructure Monitoring for all 50 states (Maximum of 2 sensors per state)	Monthly Report on sensor implementation status	Formal
2. Territory Infrastructure Monitoring for the District of Columbia and 5 Territories (Maximum of 1 sensor per territory)	Monthly Report on sensor implementation status	Formal
3. Tribe Infrastructure Monitoring for 5 of the largest member tribes (Maximum of 1 sensor per tribe)	Monthly Report on sensor implementation status	Formal
4. Elections Infrastructure Monitoring for all 50 states and 6 Territories (Maximum of 1 sensor per state and territory)	Monthly Report on sensor implementation status	Formal
5. Elections Infrastructure Monitoring for 55 localities (Maximum of 1 sensor, for largest localities in Bottom-Up and Hybrid state elections environments)	Monthly Report on sensor implementation status	Formal
6. Albert Inventory/Lifecycle Refresh Report that includes that differentiates election from no election entities.	Quarterly Report	Formal

Allowable costs under the Federal Award do not include any additional sensors or related administrative costs beyond what is listed in the deliverables above.

The Recipient must:

1. Maintain an architecture that minimally incorporates intrusion detection sensors that provide both statistical anomaly-based/behavior detection and signature detection capability with offline application programming interface for capturing network traffic (pcap processing).

2. Perform near-real time and post-collection analytics on Albert netflow and related data to identify trends and anomalous activity that helps drive improved network defense through deployed capabilities (e.g., Albert signature, MDBR domain blocking).

3. Configure, maintain, and archive event and audit log information, which includes device access logs, general systems and security logs, and application/event logs.

4. With DHS PM approval and agreement of the SLTT entity, provide IDS implementation and monitoring of SLTT networks engaged in hosting select National Special Security Events. Monitoring will be conducted for a period of 3 to 6 months in duration.

Deliverable includes:

Deliverable	Due Date	Type
Albert Alert Notification to Members	Near Real Time	Formal

4.3.5 Task 16- Endpoint Detection and Response (EDR)

The Recipient must:

1. Maintain a technology platform fused with a 24/7/365 response team to operationalize prioritized High Value/Critical SLTT/Elections Infrastructure assets with EDR capabilities. The Recipient must provide:
    - MOA(s) with participants
    - Infrastructure/capacity, engineering resources, and training needed to support the EDR solution
    - Installation assistance of Endpoint Protection Clients
    - Configuration, maintenance, and lifecycle replacement of the EDR solution
    - Configuration and maintenance of blocking policies to include ongoing rule updates
    - Monitoring, management, and analysis of deployed EDR solution
    - Timely reporting and notifications to members regarding events flagged by the EDR solution

2. Provision the following Program Phase deliverable coverage (within SLTT/Elections cloud and enterprise infrastructure):
    - Prioritize the allocation of licenses and installations to ISAC members based on risk prioritization and other criteria provided by CISA.
    - Maintain a short strategy/rationale detailing specific aspects of member deployment that will be prioritized for EDR rollout (i.e., what aspects of SLTT infrastructure, in what state/local/tribal/territorial organizations, with supporting explanation based on risk).
    - Have the capability to programmatically block malicious activity and quarantine compromised systems on behalf of the member

organizations.

- Ingest threat indicator information from the EDR solution and correlate the data for identifying prioritized threat information to support cross SLTT/Elections cyber response.
- Integrate aggregated, anonymized EDR activity data observed across membership into reporting to ISACs membership, as appropriate.
- Work with CISA to develop a short report that details lessons learned from entity use and ISAC reporting related to EDR, analysis of the effectiveness of measures deployed in preventing intrusions and malware infection (specifically focusing on ransomware), metrics detailing malicious activity observed, blocked, and prevented across participants and a recommendation on whether to continue or discontinue offering EDR as a long-term program.

Deliverable includes:

Deliverable	Due Date	Type
50,000 – 75,000 client licenses	Monthly Report on endpoint status	Formal
Quarterly Reports	Lessons Learned at each quarter program is in place	Formal

4.3.6 Task 17 –National Prevention Program

The Recipient must implement a National Prevention Program, to include Managed Email Security Gateway (Task 18) and Web Application Firewall (Task 24) functionality, as well as evolution of the Albert functionality to include block listing and intrusion prevention capabilities, as described below.

1. Recipient must implement a program of a voluntary national-level unclassified Unified Threat Management service for SLTT/Elections using behavior-based commercial technologies with government developed threat data and automation to:
    - Provide a highly available and reliable managed network security service using automated sensing and mitigation capabilities.
    - Detect, combat, and block advanced threats (to include zero-day, data loss prevention and ransomware) from entering or leaving the SLTT/Elections network
    - Enhance ISAC threat information by ingesting threat data from the security stack for correlation and analysis
    - Provide SLTT/Elections stakeholder and CISA visibility of cyber threat

activity (nation-state and malware/ransomware) and analysis

2. The program should consider models such as the Department of Defense SHARKSEER program for integrating commercial behavior-based intrusion detection/prevention and automation, as well as the CISA EINSTEIN 3 accelerated program and Enhanced Cybersecurity Services (ECS) for cost-effective traffic aggregation. Recipient shall:
    - work with CISA and partners, to maintain memorandum of agreements with ISPs or other contractors for the purpose of aggregating SLTT/Elections network data for processing via a unified threat management security stack;
    - augment protection of SLTT (including elections) infrastructure, using a wide variety of network security services ranging from IPS, URL filtering, Gateway AV, antispam, and services to combat advanced threats such as file sandboxing, data loss prevention and ransomware protection; and,
    - connect the capabilities of Web Application Firewall and Email Security to expand membership knowledge on how they interrelate.
3. Recipient must provide outreach and an initial Proof of Value service capability offering in accordance with the CIS submitted PMP in time for protecting elections.
4. As the Proof of Value is designed, operated, and evaluated, there are several questions that the Recipient must study and report on to inform whether and how a more permanent capability could be put in place in the most efficient and effective way. These areas of question include but are not limited to:
    - Model and architecture for efficiency and effectiveness
    - A cost-benefit analysis, including use of classified signatures
    - How the program could integrate or overlap with existing capabilities; scalability and cost for expanding participation
    - What protective functionality should be included
    - Cloud and encryption challenges
    - Legal and privacy challenges
    - False positives and downtime
    - Free market interference

Deliverable includes:

Deliverable	Due Date	Type
Proof of Value Report	Lessons Learned at Proof of Value Phase achievement, to be delivered no later than twelve months post Award	Formal
Program Status Report	Monthly when program is operational	Formal

4.3.7 Task 18 – Managed Email Security Gateway

The Recipient must:

1. Maintain an Email Security Gateway for SLTT and Elections that spans email applications used on desktop, laptop, and mobile devices.
2. Continue to provide protection of SLTT (foremost elections) infrastructure, using an integrated hardware and software solution, with a multilayered approach to provide managed email gateway security protection against email threats, with effective spam, virus, spoofing, phishing and spyware protection and detection, URL defense and dynamic content filtering. Processing shall be optimized to maximize performance and capability to filter millions of messages per day and leverage commercial indicators.
3. Continue to enhance security and manage visibility into email threats across SLTT/Elections for reporting purposes to members.
4. Continue to integrate aggregated, malicious threat activity observed across membership into reporting to membership via monthly calls.
5. Maintain and enhance implementation documentation and an FAQ page and provide support via the SOC and our Operations Support Team, to participating Multi-State ISAC/Elections Infrastructure ISAC members.
6. Continue to develop and distribute best practice guidance materials on secure email implementation for organizations not participating in the Managed Email Security Gateway service.

Deliverable includes:

Deliverable	Due Date	Type
Program Status Report	Monthly	Formal

4.3.8 Task 19 - Malicious Domain Blocking and Reporting

The Recipient must:

1. Work with secure DNS providers to directly ingest SLTT/Elections members blocked DNS requests.
2. Maintain a capability implemented on ISAC members' internal DNS resolvers that generates a notification of blocked DNS requests to the ISAC for reporting purposes to members.
3. Continue sourcing blocked DNS request data for reporting purposes to members.
4. Develop and maintain infrastructure/capacity and engineering resources to support data ingestion and generation of automated reports to members.
5. Maintain data ingestion, report generation, and analyst/member alerting capabilities.
6. Maintain IOC orchestration within ISAC Threat Intelligence Platform to gather insight across all members regarding DNS blocking/malicious activity.
7. Maintain aggregated, anonymized DNS blocking/malicious activity data

observed across membership into reporting to membership via monthly calls.
8. Maintain all data associated with this task according to any technical specifications that DHS/CISA may provide and share such data with DHS/CISA upon DHS/CISA's request.

Malicious Domain Blocking and Reporting Plus (MDBR+)

The Recipient must provide additional functionality to MDBR that will:

1. Support DNS-over-TLS, DNS-over-HTTPS with encryption.
2. Provide redirection or sinkholing.
3. Provide stakeholders the ability to view real time analytics of DNS environment defined by customer base.
4. Maintain the ability for stakeholder to make allowlist / blocking decisions based on organizational policy.

Deliverable includes:

Deliverable	Due Date	Type
Program Status Report (to include MDBR and MDBR+)	Monthly	Formal

4.3.9 Task 20 –Data Collection

The Recipient must:

1. Parse and normalize raw events from each telemetry data source at machine speeds.
2. Identify cybersecurity data assets collected, purchased, or generated.
3. Map Data Assets to DHS/CISA cybersecurity conceptual data model.
4. Combine structured, semi-structured, unstructured and reference data to support investigative analysis.
5. Enrich context of data elements of the normalized event and label the data with threat information cross reference checks.
6. Aggregate, store, normalize, and integrate across multiple, disparate sources of information. Examples include but not limited to:
    - Sensor threat information
    - Incident/Event threat information
    - External Data Enrichment sources, including but not limited to:
        - SLTT/Elections authorized access to results from vulnerability scans/penetration tests performed by DHS/CISA
        - SLTT/Elections Threat data identified by DHS/CISA Code and Media Analysis
        - GeoIP, WhoIS Information, Domain Look Up, etc.
        - Intelligence report/advisories

- Threat actor/group

7. Identify data assets appropriate for publication to broader public.
8. Provide data-on-demand query capability based on data that has appropriate SLTT/Elections stakeholder protections in place so that analytics could be done rapidly against large amounts of data while ensuring that users only receive results they are allowed to have.
9. Develop data asset documentation by collecting standard metadata and access control information.

Deliverable includes:

Deliverable	Due Date	Type
Data Asset Documentation	Semi-Annually	Informal

4.3.10 Task 21 – Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)

The Recipient must:

1. Leverage Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) capabilities to optimize the SOC.
2. Provide automated workflow that enables near real-time threat analytics and alerting against in-motion data to alert Analysts with a determination of risk and the decision to act.
3. Combine context-specific data with analytics and machine learning to look for suspicious patterns, correlate behaviors, and anomalies across a wider range of both historical and near real-time data.
4. Work collaboratively with CISA and other partners to implement analytics to better understand cybersecurity trends and threats.
5. Seek to reduce the mean time to detect (abbreviated MTTD) and the mean time to respond (MTTR) to cyber threats via Artificial Intelligence (AI) learning protocols like machine learning.
6. Integrate security tools, applications, and systems to enable SOC teams to automate and orchestrate mundane, time-consuming, and repetitive manual tasks.
7. Orchestrate machine-to-machine actions to align with business/operational priorities as captured in playbooks/CONOPS.
8. Inform communities of trust via bi-directional automated information sharing of prioritized threats.
9. Maintain metrics on the ratio of collected events and those analyzed for threats.
10. Provide Application Programming Interface (API) for seamless third-party integration with SLTT/Elections and CISA security tools.
11. Use SOAR capabilities to improve and grow the volume of validated

indicators that are shared with trusted communities (member feed plus AIS).

12. Leverage SOAR to enable greater automation and grow capacity to review indicators at scale and possibly consider automating the sharing without any manual validation.

Deliverable includes:

Deliverable	Due Date	Type
Automated Workflow Playbooks	Semi-Annually	Formal

4.3.11 Task 22 – Commercial Cyber Threat Feeds

The Recipient must:

1. Continue to utilize subscriptions to commercial cyber threat feeds for both the ISACs and State Fusion Centers to enable operational collaboration and sharing of intelligence reporting. The Recipient must ingest commercial cyber threat feeds as directed by CISA, in order to ensure alignment between this task and CISA's Shared Cybersecurity Services (or successor) program.
2. Continue to integrate and manage these feeds into the ISAC's threat intelligence platform(s) to enable access to additional threat context to 1) enrich understanding of observed threats, and 2) task ISACs deployed capabilities.
3. Use derivative information to enrich cyber threat intelligence advisories shared with ISAC members.

4.3.12 Task 23 – Threat Intelligence Platform (TIP)

The Recipient must:

1. Unite and integrate the SLTT/Elections cyber ecosystem through a Threat Intelligence Platform.
2. Centralize threat intelligence sharing, analysis, and investigation in a threat intelligence platform for the SLTT/Elections community of trust.
3. Provide a threat intelligence service that gathers current information related to potential attack sources that is relevant to the SLTT/Elections community of trust.
4. Provide infrastructure capacity to support bi-directional SOC and multi-tenant SLTT/Elections Analyst-to- Analyst community of trust threat indicator exchange.
5. Provide account management, audit logging and access control management for the Threat Intelligence Platform for the stakeholder community.
6. Correlate external and internal data to gain context, improve relevance of threats, and provide continuous threat context and assessments.
7. Provide threat prioritization that is calculated from across many separate sources, both external and internal, to deliver a single source of truth for the

SLTT/Elections community using the aggregated context provided.

8. Prevent tool over-load, by controlling focus on the threat data that is most relevant (high risk) and preventing stale data from being active.
9. Provide an intuitive user interface that enables SOC and SLTT/Elections Analysts to access and analyze data, collaborate, research, comment, organize, and identify an active cyber prioritized threat offense list and threat feed in near real-time. The Recipient will provide all 50 states and 50 state election offices with TIP access, including the capability to collaborate with SLTT/Elections ISAC analysts.
10. Maintain parameters that calculate a near real-time prioritized threat offense list for detailed Analyst investigation/review via the user interface and provide a downloadable file.
11. Automate the operationalization, threat modeling/characterization and use of derived threat intelligence across all SOC systems.
12. Facilitate machine-to-machine threat data-feed and exchange of prioritized indicators of compromise with the Federal government and SLTT/Elections using open standard APIs.
13. Provide support for open standards to include Trusted Automated Exchange of Indicator Information (TAXII), Cyber Observable Expression (CybOX), and Structured Threat Information Expression (STIX) - the established standards for automated indicator sharing with SLTT/Elections/DHS stakeholders.
14. Maintain a near real-time prioritized threat offense list/threat data-feed that aligns with the novel release/scoring methodology being researched within the SLTT/Elections community.

Deliverable includes:

Deliverable	Due Date	Type
One client license per state and per election entity, for a total of 100 TIP client licenses and a minimum of 8 Concurrent User licenses for DHS/CISA CSD usage to support collaborative information sharing efforts.	Monthly Report on client enrollment	Formal

4.3.13 Task 24 – Web Application Firewall (WAF)

The Recipient must:

1. Maintain an offering for Web Application Firewall (WAF) to be delivered to select SLTT organizations or communities.
2. Maintain and grow membership for the WAF to SLTTs, particularly election offices and SLTTs lacking resources to implement themselves.
3. Develop and maintain a WAF that is operational for organizations of any size to have cloud-based protection for their public facing web pages and applications by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the members application.

4. Integrate aggregated, malicious threat activity observed across membership into reporting to membership via monthly calls, advisories, or other means.
5. Develop and provide training on WAF configurations to Administrators.

Deliverable includes:

Deliverable	Due Date	Type
Program Status Report	Monthly	Formal

4.3.14 Task 25 – SLTT Critical Infrastructure Baseline Security Program

The Recipient must:

1. Maintain an SLTT Critical Infrastructure (CI) Baseline Security Program.
2. Implement an ISAC "Blue Team" Proof of Value for targeted interaction with and on-site visits to key CI SLTT/Elections.
3. Maintain an SLTT/Elections CI Dashboard and Common Operational Picture to help organizations visualize and prioritize their deployment of baseline security controls.
4. Facilitate enhanced peer-to-peer mentorship and collaboration to better leverage peer lessons-learning and best practices.
5. Provide a cross-sector and broadly encompassing information sharing and analysis capability for CI, leveraging the investments in the Multi-State ISAC.
6. Publish in-depth guidance on how to prevent initial intrusions using baseline security controls.

Deliverables include:

Deliverable	Due Date	Type
Program Status Report	Monthly	Formal

4.3.15 Task 26- SOC Incident Tracking System

The Recipient must support the Operations and Maintenance (O&M) for a SOC incident tracking system and develop strong workflow capabilities.

4.3.16 Task 27- Logging Capability

The Recipient must analyze the current logging capabilities and:

1. Ensure that available sensor traffic is logged and available for analysis in accordance with DHS/CISA and ISAC CONOPs, and with federal agency

requirements issued by CISA and/or OMB pursuant to section 8 of Executive Order 14028, including, but not limited to:

- Network Metadata collection (i.e., Enhanced Netflow/IPFIX)
- Passive Domain Name System
- IDS/Intrusion Prevention System (IPS) events
- Endpoint Detection and Response (EDR) events

2. Tune the capabilities as practicable to improve efficiency.
3. Identify shortfalls in the current capability.
4. Recommend improvements to current processes.
5. Implement filtering and/or correlation to reduce data volume and make these filters/rules available to CISA for review.

4.3.17 Task 28 - Data Retention and Storage

The Recipient must:

1. Maintain a minimum of 180 days of active (hot storage) network metadata, alert/event, indicator data and manager logs.
2. Maintain and preserve all pertinent log data involving cybersecurity incidents for evidence and review for a minimum of one year and in in accordance with prescribed governance/mandates.
3. Provide stakeholders need-to-know access to the events and network metadata/netflow in order to generate federated queries and provide data driven analysis on demand.
4. Provide ability to flag critical data for retention indefinitely.

4.4 Functional Area 4: Cyber Security Communications and Coordination

4.4.1 Task 29 - Brand Management & Key Message Development

The Recipient must clearly convey government owned SLTT and election ISAC brands messaging and products, create stakeholder unity, and establish connectivity with stakeholders.

To fulfill these priorities, the Recipient must:

1. Cultivate brand advocacy through formal stakeholder engagement programs.
2. Maintain regular ongoing meetings with SLTT/Elections Executive Committee members and relevant stakeholders to ensure approval of any new, revised, or ongoing key message development, and provide an opportunity to discuss branding matters.
3. Create clear and compelling messages that clarify joint CISA/ISAC strategy and spread across the SLTT/Elections community.
4. Connect the ISAC brand to the DHS/CISA website on ISAC disseminations, to bolster partnership affiliation, provide differentiation of services, expand attributes of service, and increase visibility of services provided to

SLTT/Elections. Co-branding processes must be cleared though CISA External Affairs first.

4.4.2 Task 30 – Stakeholder Engagement Relations

The Recipient must foster national outreach, cybersecurity awareness, preparedness, and increased collaboration among the SLTT/Elections Community and with Federal Cyber partners.

The Recipient must:

1. Manage outreach, introductions, and relationship building with SLTT/Elections stakeholder user base, ISAC community at large, SLTT/Elections Fusion Center advocates, Federal stakeholders, critical infrastructure subsectors (e.g., elections, educational institutions).
2. Assist DHS/CISA in communicating DHS/CISA capabilities to SLTT/Elections stakeholders at all times and keep the DHS/CISA PO and SLTT Partnerships Manager informed of any and all customer outreach activities.
    - Recipient must coordinate with DHS/CISA with all publications prior to them being released.
3. Provide strategic direction as relevant advertising opportunities arise in alignment with agreed upon outreach.
4. Provide continued creation of tactics and themes for marketing and outreach.
5. Ensure DHS/CISA review and input to all materials provided at outreach events describing DHS and ISAC services for SLTT/Elections community.
6. Provide continued, regular communication, meetings, and brainstorming with the SLTT and Elections Infrastructure Executive Committees, Government Coordinating Council (GCC), Sector Coordinating Council (SCC), and the Sector Risk Management Agency (SRMA), and the SLTT/Elections community at large to ensure widespread reach of outreach activities and a common understanding of the cyber risk landscape among these entities.
7. Facilitate and participate in workgroups that align with SLTT/Elections GCC and SRMA goals for the community.
8. Provide operational notifications and threshold, to include:
    - Conduct notifications to SLTT partners at DHS/CISA request
    - Under DHS/CISA guidance and request, conduct notifications to SLTT partners within 24 hours
    - Provide confirmation to appropriate CISA team(s) (Threat Hunting, JCDC Partnerships) when the notification is complete
    - Provide CISA daily updates, unless a different cadence is agreed to, on the status of notifications (i.e., responses, feedback, recommendations on next steps, etc.)
    - Develop and recommend to CISA thresholds/scoring methodology for when to engage members based on emerging vulnerabilities, incidents and campaigns, and Albert sensor traffic
9. Formalize a feedback mechanism from ISAC members to CISA, to include:
    - Develop and execute a standard process where CISA is made aware of feedback from ISAC members to include feedback on

ISAC and CISA services, products, processes messages, activities, etc.
    - Standardize format/cadence of when the feedback is shared – for example: on a monthly basis in an excel document with identifying data
    - Request the ISAC advertise the opportunity to provide feedback to the ISAC and CISA on a frequent basis (i.e., during monthly calls, after SOC or CIRT assistance, etc.)
    - Break down feedback by demographics of respondents (e.g., State, Local, Tribal, Territorial, Elections)
10. Produce guidance targeting services available to small and medium entities.
11. Ensure DHS/CISA involvement with ISAC Executive Committees (ExCom):
    - DHS/CISA will have final approval of all ISAC charters prior to distribution
    - Recipient will ensure DHS/CISA are included in regularly scheduled meetings with each ExCom
    - Formalizing a feedback mechanism for ExCom members to CISA (see above)

4.4.3 Task 31 – Public Relations

The Recipient must:

1. Distribute press releases to trade publications, trade/business organizations, community groups/advocates, and general news outlets that are vetted through the DHS/CISA Program Manager and CISA External Affairs Manager.
2. Vet media inquiries, as well as facilitate and coordinate media opportunities, interviews, and tours, through DHS/CISA Program Manager and CISA External Affairs Manager.

4.4.4 Task 32– Homeland Security Information Network (HSIN)

The Recipient must:

1. Implement a HSIN communications strategy for the SLTT/Elections communities of interest.
2. Manage presence to provide relevant cyber situational awareness, collaboration, consistent messaging, and relevant content, and a means to store and share information, and send alerts and notices.
3. Maintain refreshed and additional content development and postings of relevant SLTT/Elections cybersecurity materials and coverage of events.
4. Provide outreach to, and integration with, information sources to vet SLTT/Elections members for the HSIN SLTT/Elections communities of interest.
    - Provide account and access control management services for SLTT/Elections members.
5. Maintain a 24x7x365 National Alert Map, which provides a globalized view of the dynamic cybersecurity threat landscape for the SLTT sector and its critical infrastructure sub-sectors (to include at minimum a view of the Elections sub-sector).

6. Establish a National Cyber Situational Awareness Room, an online forum during significant events for vetted individuals to participate in real-time, secure information sharing, and collaboration on issues impacting the cyber landscape.

4.4.5 Task 33 - Maintain Membership/Contact Information Collection System

The Recipient must:

1. Track and maintain current contact information and organizational affiliation for all members.
2. Encourage each organizational entity to maintain a Principal Representative for event/incident contact.
3. Track and maintain organizational profiles that include, but are not limited to: memoranda of understanding, service level agreements, SLTT/Elections log-on consent banners/notices/terms-of-use or user agreements/certification, cyber incident escalation contact information, and inventory and network configuration documentation.
4. Provide members customized service and product enrollment, with profiles to track ISAC services utilized by organizational entity and by critical infrastructure subsector.
   Implement workflow to share Stakeholder Profiles in a format sharable with DHS/CISA.
5. Maintain up-to-date records of membership in accordance with organizational change.

Deliverable includes:

Deliverable	Due Date	Type
Notice and Consent Certifications	At Service Provisioning / continuously maintained	Formal
Membership/Incident Escalation Contact Information	Monthly	Formal

4.4.6 Task 34 – Assess Current SLTT/Elections Cybersecurity Level of Maturity

The maturity of existing SLTT/Elections cybersecurity operations is a measure of effectiveness in providing the necessary threat management capabilities to protect the organization. Maturity levels will be assessed along a scale of increasing maturity from initial base capabilities to an optimized environment. The Recipient must:

1. Conduct the SLTT/Elections Foundational Assessment to assist SLTT members in preparation for completing the Nationwide Cybersecurity Review (NCSR).

2. Annually conduct the SLTT/Elections Nationwide Cybersecurity Review (NCSR) to benchmark the level of cybersecurity maturity and provide a criticality analysis across the SLTT/Elections community and its sub- sectors.
3. Provide SLTT/Elections with a standardized cybersecurity self-assessment methodology that measures enterprise-wide cybersecurity posture.
4. Ensure the assessment aligns security controls against a full set of industry best practices (e.g., NIST Cybersecurity Framework (CSF) Functions and Categories) and is based on a mutually agreed upon cybersecurity maturity model.
5. Provide the SLTT/Elections entities a scorecard that measures SLTT/Elections conformance to security controls.
6. Provide the SLTT/Elections entities a risk profile that identifies prioritized gaps in capabilities.
7. Provide the SLTT/Elections entities metrics to determine how they rate in maturity as compared to similar organizations across the maturity model.
8. Provide specific and actionable mitigation recommendations to SLTT/Elections entities.
9. Author and submit to the DHS/CISA PO and SLTT Partnerships Manager an annual report that details the results of the NCSR. Report is due 90 working days after the survey close-out date.
    - An Executive Summary and Final report on SLTT/Elections cybersecurity posture will be briefed by CISA to Congress on a biennial basis.
10. Provide an insightful cybersecurity maturity model and compliance reporting.
11. Submit an annual executive summary report of SLTT/Elections findings to DHS/CISA Program Manager and SLTT Partnerships Manager within 80 working days after the survey close-out date.
12. Upon CISA's request, provide notice to SLTT entities taking the NCSR that their responses are not anonymous.
13. Upon CISA's request, provide individual SLTT entity NCSR responses to CISA.

Deliverable includes:

Deliverable	Due Date	Type
Final Draft NCSR Report, Cover Letter for Transmittal to Congress, and NCSR Executive Summary Briefing	80 days after survey close	Informal
Foundational Assessment Report	Annually	Formal

4.4.7 Task 35 – Training and Education

To help cultivate and promote cyber education activities s that create a vibrant cyber SLTT/Elections workforce who understand risks and stay ahead of emerging threats,

the Recipient must:

1. Publicize the Federal Virtual Training Environment (FedVTE) on-demand cybersecurity training system that is available at no charge for SLTT, and federal government personnel.
2. Vet SLTT/Elections members for the FedVTE program and provide account management services for SLTT/Elections members.
3. Publicize resources available through the National Initiative for Cybersecurity Careers and Studies (NICCS).
4. Publicize the Cybersecurity Awareness Month activities to raise awareness about the importance of cybersecurity.
    - Engage the SLTT communities to issue proclamations or letters of support for the Cybersecurity Awareness Month.
    - Engage the SLTT/Elections communities to promote use of campaign toolkit resources to support spreading the word about cybersecurity.
    - Complement DHS's month-long "key messages" by distributing theme-based awareness materials and scheduled event information to SLTT/Elections members.
    - Co-sponsor and/or publicize DHS/CISA Cybersecurity educational webinars, videos, and podcasts.
5. Publicize a training calendar of scheduled training opportunities.
6. Provide ISAC membership and user profile maintenance training.
7. Train SLTT/Elections cyber threat analyst members quarterly using techniques that build on the use of the threat intelligence platform as the key tool to convey the tradecraft of cybersecurity threat intelligence.
8. Co-sponsor and/or publicize DHS/CISA National Cybersecurity Educational Webinars, Videos, and Podcasts.
9. Provide members a means for customized training and awareness product enrollment and delivery, and distribute awareness products, including but not limited to:
    - Intelligence Products: Threat intelligence assessment reports on malware campaigns that include adversary tools, tactics, and procedures (TTP), and mitigation steps.
    - Cybersecurity Spotlights: Share cybersecurity awareness information on timely, relevant, and actionable information of broad interest.
    - Cyber News Bulletins: Share summaries of open-source cyber reporting topics that may be of broad interest to SLTT/Elections communities (e.g., on election security).
    - Federal Binding Operational Directive (BOD) translations into guidance consumable for SLTT/Elections government partners: Share intent of DHS safeguards that are being implemented on Federal information and information systems to support awareness of critical cybersecurity actions.
10. Show the impact CISA Cyber Security Awareness Campaign Grantee's activities have on the advancement of DHS goals through cumulative quarterly datasheet reporting of the following performance metrics:

- Secure federal civilian networks
  - Number and list of Cybersecurity Awareness Campaign key messages offered related to Federal Civilian Networks cybersecurity activities.
  - Types of Cybersecurity Awareness Campaign outreach engagements/instances targeted toward the Federal stakeholder audience
  - Number of Federal Departments reached through Cybersecurity Awareness Campaign messaging
  - Actual or estimated number of Federal stakeholders reached through each type of outreach engagement/instance
- Strengthen the security and resilience of critical infrastructure
  - Number and list of Cybersecurity Awareness Campaign key messages offered related to cybersecurity activities specific to critical infrastructure information technology systems and/or infrastructure control systems security
  - Types of Cyber Security Awareness Campaign outreach engagements/instances targeted toward the critical infrastructure security stakeholder community
  - Actual or estimated number and demographic of critical infrastructure security community stakeholder groups reached through each type of outreach engagement/instance sorted by Critical Infrastructure Sector, CISA Region, State, Local, Tribal, Territorial, Private Sector, and international affiliation
- Assess and counter evolving cybersecurity risks
  - Number and list of Cybersecurity Awareness Campaign key messages offered related to cybersecurity assessing and countering cybersecurity risks
  - Types of Cyber Security Awareness Campaign outreach engagements/instances targeted toward assessing and countering cybersecurity risks
  - Actual or estimated number and demographic of community stakeholder groups reached through each type of outreach engagement/instance sorted by CISA Region, Federal State, Local, Tribal, Territorial, Private Sector, and international affiliation
- Build a national culture of preparedness
  - Number and list of Cybersecurity Awareness Campaign key messages related to general public computer user cybersecurity preparedness activities
  - Types of Cybersecurity Awareness Campaign outreach engagements/instances targeted toward the general public computer user audience
  - Actual or estimated number of general public computer users reached through each type of outreach engagement/instance
  - Number and types of Cybersecurity Awareness Campaign measurement tools used to collect short and long-term effects of national understanding of individual roles in cybersecurity

and changes in behavior toward enhanced cybersecurity among campaign participants.
    - Actual number and demographic of community stakeholder groups/participants assessed through Campaign implementation of behavior change measurement tools, sorted by CISA Region, Federal, State, Local, Tribal, Territorial, Private Sector, and international affiliation.
    - Actual number of responses received (per each measured category) from each behavior change measurement tool implemented through the Cybersecurity Awareness Campaign.
    - Percentage increase in the total number of Americans and International users receiving overall cybersecurity awareness campaign messaging from previous campaign years.
- Support outcome-driven community recovery
    - Number of Cybersecurity Awareness Campaign key messages offered related to specific community recovery activities following a cybersecurity incident
    - Types of Cybersecurity Awareness Campaign outreach engagements/instances targeted toward the cybersecurity community recovery audience
    - Actual or estimated number and demographic of community recovery stakeholders reached through each type of outreach engagement/instance, sorted by CISA Region, Federal, State, Local, Tribal, Territorial, Private Sector, and international affiliation.
    - Number of new DHS partnerships formed through Cybersecurity Awareness Campaign activities

Deliverable includes:

Deliverable	Due Date	Type
CISA Cyber Security Awareness Campaign Performance Metrics	Annually	Formal

4.4.8 Task 36 - Best Practice Cybersecurity & Privacy Documentation

The foundation for an organization's cybersecurity and privacy program is its policies and standards. To support establishment of SLTT/Elections governance materials that align with leading best practices, the Recipient must:

1. Develop and maintain editable best-practice enterprise class policies, standards, and metric templates that the SLTT/Elections communities are able to tailor to their organization's needs.
2. Provide Best Practice Templates that align with leading best practices, to include the NIST Cybersecurity Framework.

3. Leverage the SLTT/Elections communities to work together on the templates to provide templates that are living documents available to the entire membership community.

Deliverable includes:

Deliverable	Due Date	Type
Best Practice Templates	Update Semi-Annually	Formal

4.4.9 Task 37–Annual SLTT/Elections Membership Meeting

To facilitate SLTT/Elections members' ability to stay abreast of the latest best practices, trends, and research findings that affect day-to-day responsibilities and to foster enhancement of cybersecurity program performance and maturity, the Recipient must:

1. Organize and manage all aspects of planning and execution of an annual membership meeting to bring together SLTT/Elections colleagues from across the country, along with industry experts and key government officials and stakeholders, including but not limited to:
    - Crafting an initial meeting plan with costs to be submitted to CISA PO no less than 90 days before meeting. Plan to include:
        i. Venue
        ii. Revised budget projection with the venue discount, if applicable
        iii. List and number of the entity types expected to attend, with percentages of the total attendance (e.g., K-12 10%, health care 5%, state government 60%, etc. provided)
        iv. The Meeting and Event Registration Platform being used, and associated costs
        v. Proposed Agenda/tracks/themes/panels
        vi. Number/types/costs for signage needed at the event
        vii. Televising options (will it be recorded, streamed live?)
        viii. Press attended (closed or open)
        ix. Advertisement strategy, to include timeline
    - Submitting a final meeting planning package to DHS/CISA no less than 30 days before meeting that includes the finalized information listed above, as well as at minimum the meeting itinerary, speaker lineup, and advertising
    - Marketing
    - Management of registrants
    - Comparison of venues and services to identify a venue decision

- Any costs above DHS/CISA approved budget will be borne by the Recipient

2. Provide members with opportunities to connect and share information on cybersecurity trends and glean insight to increasing the common mission purpose of enabling innovation, education, workforce development, enhanced cyber readiness, and resilience.
3. Provide peer group collaboration to share best practices and lessons learned and serve as a forum for networking and engaged discussions on mission need.
4. Provide an After Actions Review with lessons learned to include budget and expenditure information from the Annual SLTT/Elections Membership Meeting no later than 60 days after the close of the meeting.

4.4.10 Task 38-CISA Cybersecurity Summit and Awareness Campaigns

To facilitate SLTT/Elections members' ability to stay abreast of the latest best practices, trends, and research findings that affect day-to-day responsibilities and to foster enhancement of cybersecurity program performance and maturity, the Recipient must:

1. Partner with CISA in the planning of CISA Cybersecurity Summit and Cybersecurity Awareness Campaigns to bring together the SLTT/Elections colleagues from across the country, along with industry experts and key government officials and stakeholders.
2. At CISA's request, provide two planners in support of an SLTT and Elections-focused track or programming at the CISA Cybersecurity Summit.
3. At CISA's request, planners will elicit participation in panels and speaking roles from amongst ISAC membership and coordinate with CISA planners in building out the agenda and coordinating logistics for these sessions. These sessions will be approved by CISA and focus on providing an opportunity for the exchange of ideas related to SLTT and election entity cybersecurity topics.
4. At CISA's request, planners will also work with CISA to develop a networking event for ISAC membership at the CISA Cybersecurity Summit.
    - Providing opportunities to connect and share information on cybersecurity trends, glean insight to increasing the common mission purpose of enabling innovation, education, workforce development, and enhanced cyber readiness and resilience.
    - Providing SLTT/Elections peer group collaboration to share best practices and lessons learned and serve as a forum for networking and engaged discussions on mission need.
5. In addition to participation by the planners, Recipient will plan for at least one member of the LNO team in addition to a member of the SOC or CERT and a member(s) of leadership to be present at CISA Cybersecurity Summit for its duration.
6. Have the planners participate in cybersecurity awareness campaign interagency planning working groups to provide advice, review, and comment on campaign materials to support development of SLTT and Elections-focused cybersecurity content or products.

4.4.11 Task 39– Cyber Exercises

The Recipient must:

1. Participate in planning meetings (virtual or in-person) and audio/conference calls as needed in support of DHS/CISA cybersecurity exercises.
2. Participate, coordinate, observe, and provide a threat brief as requested for DHS cybersecurity exercises related to risk mitigation and recovery around realistic scenarios.
3. Ensure Incident Response CONOPs are developed and maintained.
4. Provide coordination with SLTT/Elections community membership to support cybersecurity exercise awareness and lessons learned.
5. Develop 5-minute cyber tabletop exercises to share as part of activities of Business Continuity/Cyber Exercise Working Group for conducting on Monthly Membership Calls.

4.4.12 Task 41 - Other duties as assigned consistent with Joint Explanatory Statement (Optional)

At CISA's direction, Recipient must carry out other duties as assigned consistent with Title III of Division F of the Joint Explanatory Statement accompanying the Consolidated Appropriations Act, 2023 (P.L. 117-103).

State, Local, Tribal and Territorial (SLTT)

Security Operations Center (SOC) |
Information Sharing and Analysis Services
(ISAC)

Program Work Supplemental Scope – Appendix B

Programs and Initiatives

Supports	Program/ Initiative Name	Program/Initiative Description
Both MS-ISAC and EI-ISAC	Data Warehouse	MS/EI-ISAC uses a Date Warehouse that allows for a minimum of 180-day storage and provides members with the capability to conduct queries against a wide variety of data.
Both MS-ISAC and EI-ISAC	Cyber Incident Response Team (CIRT)	CIRT provides technical expertise to manage, coordinate response and remediation communications, document, and report computer security incidents.
Both MS-ISAC and EI-ISAC	Security Operations Center (SOC)	A 24x7x365 Security Operations Center (SOC) that provides real-time cybersecurity event monitoring, synthesizing, and analyzing threats directed at the SLTT sectors, and their critical infrastructure sub-sectors.
Both MS-ISAC and EI-ISAC	Cyber Threat Liaisons (CTL) Analysts	CTL analysts are TS/SCI cleared and embedded within CISA Threat Hunting. CTL analysts are responsible for conducting analysis, providing time-sensitive cybersecurity information, collaboration services, etc. Embedded CTL Analysts enhance the quality and efficiency of analytic support and incident response support to SLTT government partners.
Both MS-ISAC and EI-ISAC	Education & Training	Cultivation and promotion of cyber education initiatives that help create a vibrant cyber SLTT workforce that understands risks and stays ahead of emerging threats.
Both MS-ISAC and EI-ISAC	Classified Facility & Security Operations (SCIF)	MS/EI-ISAC maintains a certified sensitive compartmented information facility (SCIF) to process classified information and facilitate collaboration.
Both MS-ISAC and EI-ISAC	Stakeholder Engagement	The fostering of national outreach, cybersecurity awareness, preparedness, and increased collaboration among the SLTT community and Federal Cyber partners.
Both MS-ISAC and EI-ISAC	Threat Intelligence Platform (TIP)	A TIP is an essential capability in the correlation, enrichment, and verification of intelligence information to ensure that any knowledge shared is accurate, timely, and relevant. The TIP project is centered on modernizing the MS/EI-ISAC TIP environment, developing a real-time intelligence sharing architecture for members to gain trusted, vetted, and verified CTI, and building a collaborative environment for members to maintain situational awareness of the threat landscape.

Supports	Program/ Initiative Name	Program/Initiative Description
Both MS-ISAC and EI-ISAC	Endpoint Detection & Response (EDR)	EDR is a software-based technology solution to protect servers and workstations from cybersecurity threats. It is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.
Both MS-ISAC and EI-ISAC	Albert Intrusion Detection Capability and Lifecycle Management	Albert is an IDS designed specifically for SLTTs with enhanced support from the MS/EI-ISAC SOC. Albert typically sits within the perimeter firewall, monitoring an entity's Internet connection, collects network data, and sends it to the MS/EI-ISAC for analysis.
Both MS-ISAC and EI-ISAC	Annual Meeting (Stakeholder Engagement)	MS/EI-ISAC, along with CISA, hosts an annual membership meeting that center on sharing ideas about how to improve the cybersecurity posture of SLTT governments, as well as our critical election infrastructure.
Both MS- and EI-ISAC	Malicious Domain Blocking & Reporting (MDBR)	MDBR program has been instituted to prevent IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block most ransomware infections just by preventing the initial outreach to a ransomware delivery domain. It delivers a security-focused DNS service to SLTT governments, via the Akamai Enterprise Threat Protector platform.
Both MS- and EI-ISAC	Malicious Domain Blocking & Reporting Plus (MDBR+)	MDBR+ is an expansion of the MDBR service to provide members with Web-based access to their DNS activity dashboard, the ability to create acceptable usage policies, custom error pages, plus allow and deny lists. The expanded features support internal investigations, regulation compliancy audits and improved security awareness training.
Both MS-ISAC and EI-ISAC	Web Application Firewall (WAF)	Provide an easy to implement web application firewall offering that gives MS/EI-ISAC members protection against HTTP-based inbound attacks and DDOS protection.
Both MS- and EI-ISAC	Nationwide Cybersecurity Review (NCSR)	NCSR measures maturity according to the NIST CSF function areas and categories to provide insight on the level of maturity and risk awareness of SLTT governments information security programs. The assessment allows members to compare their maturity to similar organizations and facilitate a self-comparison year-to-year.
Both MS-ISAC and EI-ISAC	Email Security Managed Service	Provide an easy to implement email security offering that gives members an additional layer of protection against malicious inbound email attacks and threats. Provide members with best practices guidance for DMARC and Microsoft Office 365 email service configurations.

Supports	Program/ Initiative Name	Program/Initiative Description
EI-ISAC	Coordinated Vulnerability Disclosure Program for SLTT Elections Offices (VDP)	A formalized process to receive, validate, and transmit vulnerability information from known security researchers to the appropriate elections' office. This provides a trusted forum for sharing and remediation of vulnerability information, the lack of which has led to public disclosure through conferences and media reporting without an opportunity for SLTTs to remediate or address.
Both MS-ISAC and EI-ISAC	National Alert Map and Situational Alert Map	Two maps: the first is National Alert Map; housed on the Homeland Security Information Network (HSIN) and requires States to update their status manually; the second is the Situational Alert Map, which is housed in the Security Operations Center (SOC) and provides both an automated update functionality as well as the option for States to update their status manually.
Both MS-ISAC and EI-ISAC	Security Information and Event Management (SIEM) and Security Orchestration Automation and Response (SOAR)	SIEM implements advanced analytics, including machine learning (ML), to detect and prioritize security events in an ever-increasing data set more efficiently. SOAR workflows automate analysis activities and SOC processes, freeing up analysts to perform advanced investigations instead of manually intensive tasks and procedures. The combination of capabilities enables the SOC to triage, investigate, and respond to current cyber threats actively targeting SLTT members in cyber relevant time.
Both MS-ISAC and EI-ISAC	National Prevention Program (NPP)	NPP will allow organizations of any size to have a cloud-based security stack providing core prevention, detection, response, and remediation capabilities. The NPP will include the functionalities described under Email Security Managed Service and Web Application Firewall, plus expansion of Albert to include blocklisting (Intrusion Prevention) capabilities.

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

This cooperative agreement funds and sets out the terms and conditions governing a collaborative effort between CISA and the Recipient in the execution of Award Number: xxxxxxxx

In addition to the **DHS Standard Terms and Conditions,** the following Terms and Conditions apply specifically to this Award as administered by the DHS Grants and Financial Assistance Division (GFAD):

ARTICLE I. GENERAL ADMINISTRATIVE TERMS AND CONDITIONS

A. AWARD SPECIFIC TERMS AND CONDITIONS

1. Incorporation via Reference

   a. The Additional Details, Objectives, and Performance Metrics outlined in Notice of Funding Opportunity DHS-23-CISA-123-ISAC000001, and Appendices are hereby incorporated via reference into the Terms and Conditions of this Award.

2. Award Restrictions

   Of the total funds Awarded, $*1,000,000 is* restricted from use. The Recipient must use the Program Management or the Project and Portfolio Management categories to incur expenses for planning activities related to the following restricted funds. The restricted funds may only be used once approved by CISA Program Officer (PO).

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

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

3. Project Milestones, Deliverables, and Timelines

   a. Changes to the Details, Objectives, Performance Metrics, and timelines outlined in Appendix A are subject to CISA PO review and prior approval. Any changes initiated or proposed by the Recipient should be submitted via email to the CISA PO for review and approval along with a

programmatic justification and budget impact statement.

b. The Recipient-submitted Program Management Plan (PMP) establishes technical milestones and deliverables. If the Recipient fails to achieve two or more technical milestones and deliverables, CISA PO may request modifications to the PMP. In the alternative, CISA PO may deem the Recipient's failure to achieve these technical milestones and deliverables to be material noncompliance with the terms and conditions of this Award and take action to require a Corrective Action Plan, reduce or restrict funding, or suspend or terminate the Award.

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

5. Monthly In-Progress Review (IPR) and Quarterly Program Management Review (PMR)
   a. In addition to what is stated in Appendix A and Appendix B, slides for the monthly IPR must contain accurate and up-to-date information (including but not limited to financial information, operational data, and program status) and be sent to CISA PO at CISA.CSD.JCDC_MS-ISAC@cisa.DHS.gov no later than the 15th of the month and reflect the previous month's data. Additionally, a knowledgeable representative from Recipient shall be on the IPR calls to answer questions regarding the presented slides.

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

B. AMENDMENTS AND REVISIONS

1. Budget Revisions

   a. Transfers of funds between direct cost categories in the approved budget when such cumulative transfers among those direct cost categories exceed ten percent of the total budget approved in this Award require prior written approval by the CISA PO and DHS Grants Officer.

   b. All requests for budget revisions requiring prior approval under 2 C.F.R. § 200.308 must be submitted to the CISA PO and DHS Grants Officer.

c. To avoid expenditures on products and services duplicating CISA capabilities or products/services that are already commercially available, the Recipient must obtain the written approval from CISA PO prior to the development of new services delivered to SLTT stakeholders that are not outlined in the approved budget or are otherwise commercially available. CISA PO reserves the right based on project milestones and/or timelines to require the use of commercially available products/services in order to achieve cost and time efficiencies.

d. The Recipient is not authorized at any time to transfer amounts budgeted for direct costs to the indirect costs line item or vice versa, without prior written approval of the DHS Grants Officer.

2. Extension Request

a. The Recipient must submit all requests for extensions to the Period of Performance to the PO and Grants Officer for consideration sixty (60) days before the expiration date of the Period of Performance.

b. Requests for time extensions to the Period of Performance will be considered but will not be approved automatically and must be supported by adequate justification to be processed. The justification is a written explanation of the reason or reasons for the delay; an outline of remaining resources/funds available to support the extended Period of Performance; and a description of performance measures necessary to complete the project. Without performance and financial status reports current and justification submitted, the PO and Grant Officer will not process extension requests.

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

C. FINANCIAL REPORTING

1. Financial Reporting Accounting - the Recipient must provide a clear composition of their spending within the core services, shared services/required functionalities, and programs. The clear breakdown of these funds should be applied to the following, but not be limited to: In-Progress Reviews (IPRs), Program Management Reviews (PMRs), ABC reports, Quarterly Federal Financial Reports, Semi-Annual Federal Financial Reports, Final Federal Financial Reports. The Recipient must work with the PO to define an agreed-upon template for reporting fiscal year's financial breakdowns that will include at minimum cumulative expenditures, monthly expenditures, and monthly forecasts.

2. The Federal Financial Report (FFR) form is available online at: SF-425 *OMB #4040-0014.*

3. Semi-Annual Federal Financial Reports - the Recipient must submit a Federal Financial Report (SF425) to the DHS/CISA Grants Officer no later than 30 days after the end of the reporting period end date. Reports are due on 4/30 and 10/31. The report must be submitted electronically via www.GrantSolutions.gov. Please select the FFR submission guidance found here: https://www.Grantsolutions.gov/support/granteeUsers.html .

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

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

D. PERIOD OF PERFORMANCE

The approved Period of Performance and Budget Periods for the Award is contingent on the following:

1. Acceptable performance under the Award as determined by DHS/CISA;

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

3. Availability of appropriated funds.

E. PERFORMANCE REPORTS

1. Quarterly Performance Reports - the Recipient must submit performance reports to the DHS/CISA Grants Officer no later than 30 days after the end of the reporting period end date. Reports are due on the following dates: 01/31, 04/30, 07/31 and 10/31. The report must be submitted via GrantSolutions using the Help/Support Reference entitled, Grant Recipient Process: Performance Progress Reporting.

2. Performance reports must provide information on the overall progress by quarter and by fiscal year.These reports must include:
    i. A summary that clearly differentiates between activities completed under the SLTT SOC|ISAC cooperative agreement and related activities completed with other sources of leveraged funding.
    ii. Performance Metric Reporting as outlined in Appendix A Task 10.
    iii. A summary and status of approved activities performed during the reporting period; a summary of the performance outputs/outcomes achieved during the reporting period; and a description of problems encountered during the reporting period that may affect the project schedule.
    iv. A comparison of actual accomplishments with the goals and objectives established for the period in the DHS/CISA-approved workplan.
    v. Difficulties encountered and reasons why established objectives were not met, if applicable.
    vi. An update on project schedules and milestones, including an explanation of any discrepancies from the DHS/CISA-approved workplan.
    vii. A discussion of expenditures and financial status for each workplan task, along with a comparison of the percentage of the project completed to the project schedule and

an explanation of significant discrepancies shall be included in the report.

viii. A budget recap summary table with the following information: current approved project budget; DHS/CISA funds drawn down during the reporting period; costs drawn down to date (cumulative expenditures); program income generated and used (if applicable); and total remaining funds.

ix. Other pertinent information including, when appropriate, any discrepancies in the budget from the DHS/CISA-approved workplan, analysis and explanation of cost overruns or high unit costs.

x. For the quarterly performance reports, provide a high-level comparison between the last quarterly report and the current reporting period.

xi. At the end of the fourth quarter provide both a fourth quarter performance report and an Annual Summary Performance Report.

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

4. In accordance with 2 C.F.R. § 200.329(e)(1), the Recipient will inform DHS/CISA via email, as soon as problems, delays, or adverse conditions become known which will impair the ability to meet the outcomes specified in the DHS/CISA-approved workplan.

5. Final Performance Report - the Recipient must submit the Final Performance Report to the DHS/CISA Grants Officer no later than 120 days after the expiration of the Period of Performance. The report must be submitted via GrantSolutions using the Help/Support Reference entitled, Grant Recipient Process: Performance Progress Reporting.

F. EQUIPMENT

1. Title to equipment acquired by the Recipient under this Award will vest inthe Recipient, subject to the conditions pertaining to equipment in the 2 C.F.R. Part 200.

2. The Recipient will submit a master list of all CISA funded equipment within 90 days of Award. Master list will include all required inventory information listed in sub paragraph 4.

3. The Recipient must obtain prior written approval from DHS/CISA before purchasing equipment as detailed in 2 C.F.R. § 200.439.

4. The Recipient must submit a quarterly equipment report broken down into the following categories: SLTT/Elections (equipment used for both SLLT and election infrastructure services), Elections-specific (equipment solely used for election infrastructure) and Management (equipment used by Recipient to manage the cooperative agreement). The report will contain a description of the property; manufacturer model number, serial number, or other identification number; the source of property; name on title; acquisition date; and cost of the unit; the address of use; operational condition of the property; and, disposition data, if applicable. Disposed equipment is to remain on the inventory report. This report will be maintained and due with the Quarterly Performance Reports, and must be submitted

electronically via www.GrantSolutions.gov using the Grant Note feature and guidance found here: https://www.grantsolutions.gov/support/granteeUsers.html

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

G. PAYMENT

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

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

ARTICLE II. GENERAL TERMS AND CONDITIONS

A. ACCESS TO RECORDS

1. The Recipient and subrecipients must retain financial records, supporting documents, statistical records, and all other records pertinent to the Award or subaward for a period of three years from the date of submission of the final expenditure report pursuant to 2 C.F.R. § 200.334. There are various **exceptions** to the aforementioned record retention requirement set forth in 2 C.F.R. § 200.334,:

2. DHS/CISA, the Inspector General, Comptroller General of the United States, or any of their duly authorized representatives, have the right of timely and unrestricted access to any documents, papers, or other records of the Recipient and subrecipients that are pertinent to this Award, in order to make audits, examinations, excerpts, transcripts and copies of such documents. This right also includes timely and reasonable access to Recipient and subrecipient personnel for the purpose of interview and discussion related to such documents. The rights of access in this Award term are not limited to the required retention period but last as long as the records are retained.

3. The Recipient will include in any subaward the requirements of this Award term (Access to Records).

B. COMPLIANCE ASSURANCE PROGRAM OFFICE TERMS AND CONDITIONS

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

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

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

C. SECURITY REQUIREMENTS

Recipient access to classified information, Controlled Unclassified Information, and Sensitive But Unclassified information may be required under this Award. The maximum level of classification is Top Secret/SCI. The details will be specified in a Departmentof Defense (DD) Form 254.

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

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

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

1. EMPLOYMENT ELIGIBILITY

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

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

2. CONTINUED ELIGIBILITY

a. The PO may require the Recipient to prohibit individuals from working on this Award if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to carelessness, insubordination, incompetence, and/or security concerns.

b. If a prospective employee is found to be ineligible for access to Government facilities or information, the PO will advise the Recipient that the employee shall not continue to work or to be assigned to work under the Award.

c. The Recipient must report any adverse information coming to their attention concerning employees under the Award to DHS/CISA Security Office. Reports based on rumor or innuendo should not be made.The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report must include the employee's name and social security number, along with the adverse information being reported.

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

3. FITNESS DETERMINATION

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

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

4. BACKGROUND INVESTIGATIONS

Recipient employees (to include applicants, temporary, part-time, and replacement employees) under the Award, needing access to sensitive information, will undergo a position sensitivity analysis based on the duties

each individual will perform on the task order. All of the Recipients' employees will be required to undergo CISA fitness investigation. PIV cards will be required for all staff assigned to government facilities under this Award. The Program Office will provide the employees with the proper security paperwork for obtaining the PIV cards and will ensure that all PIV cards are returned at the end of the cooperative agreement. The results of the position sensitivity analysis will identify the appropriate background investigation to be conducted.

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

b. Required forms will be provided by CISA at the time of Award. Only complete packages will be accepted by the Security Office. Specific instructions on submission of packages will be provided upon Award.

c. Be advised that unless an applicant requiring access to sensitive information has resided in the US for three (3) of the past five (5) years, the Government may not be able to complete a satisfactory background investigation. In such cases, CISA retains the right to deem an applicant as ineligible due to insufficient background information.

d. The use of non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this Award for any position that involves access to or development of any CISA IT system or access to Federal sensitive information. CISA shall not approve LPRs for employment on this Award in any position that requires the LPR to access or assist in the development, operation, Management, or maintenance of CISA IT systems and/or sensitive information. By signing this Award, the Recipient agrees to this restriction. In those instances where other non-IT requirements contained in the Award can be met by using LPRs, those requirements shall be clearly described.

5. The security requirements for this Award order include:
    a. Personnel security
    b. Information technology security
    c. Facility security

6. The following security clauses are incorporated by reference:
    a. FAR 52.204-2, Security Requirements (MAR 2023)
    b. FAR 52.204-9, Personal Identity Verification of Contractor Personnel (MAR 2023)
    c. HSAR 3052.204-71, Contractor Employee Access (SEP 2012), ALTERNATE I (SEP 2012)
    d. Safeguarding of Sensitive Information (MAR 2015)
    e. Information Technology Security and Privacy Training (MAY 2020)

D. COMPLIANCE WITH INFORMATION SYSTEMS SECURITY

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

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

1. The Recipient must ensure that this provision is expressly incorporated into any and all contracts or subordinate agreements issued in support of this Award.

2. The Recipient represents that it will implement the security measures required by the Federal Information Security Modernization Act of 2014, including those measures detailed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 1 "Protecting Controlled Unclassified Informationin Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) (NISTSP 800-171) and are in effect at the time the Award is issued.

3. a. If the Recipient proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the Award is issued, the Recipient must submit to the Program Officer, for consideration by the CISA Chief Information Security Officer (CISO), a written explanation of—

    i. Why a particular security requirement is not applicable; or

    ii. How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

   b. An authorized representative of the CISA CISO will adjudicate offeror requests to vary from NIST SP800-171 requirements in writing. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting Award.

4. The Recipient agrees that when collecting and managing data under this cooperative agreement, it will protect the data by following all applicable state law cybersecurity requirements.

5. If the Recipient intends to use an external cloud service provider to store, process, or transmit any covered Government information in performance of this Award, the Recipient must require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/documents-templates/) and that the cloud service provider complies with requirements of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment. These measures may be addressed in a system security plan.

6. CISA will ensure that any connections between the Recipient's network or information system and CISA networks used by the Recipient to transfer data under this cooperative agreement are secure. For

purposes of this Section, a connection is defined as a dedicated persistent interface between an Agency IT system and an external IT system for the purpose of transferring information. Transitory, user-controlled connections such as website browsing are excluded from this definition. The Recipient agrees to ensure that any connections meet DHS/CISA security requirements, including entering into Interconnection Service Agreements as appropriate. This condition does not apply to manual entry of data by the Recipient into systems operated and used by DHS/CISA's programs for the submission of reporting and/or compliance data.

7. Supply Chain Risk

a. Government reserves the right to complete a review of the supply chain risk and conduct a risk assessment at any time during this Award. Such risk assessment may include reviewing any contractors, suppliers, distributors, and manufacturers involved in the Awardee's supply chain. Upon written notification from government, within 10 days or a reasonable amount of time as determined by the Grants Officer, the Recipient must provide any information government deems necessary to facilitate its Supply Chain Risk Assessment. If the Recipient believes that the information government requests contain confidential information, the Recipient may state its justification for designating the information as confidential and request that government and any third-party vendor it may use sign a confidentiality agreement before releasing the information. Designation of information as confidential does not give the Recipient the right to withhold the information. As deemed necessary, government may contract with a third party to assist in the review of the supply chain risk assessment.

Government may request the following information (or other information if deemed necessary) from the apparent Awardee:

i. The identity of the apparent Awardee's parent and/or subsidiary corporate entities.

ii. The identity of any proposed contractors (including but not limited to suppliers, distributors, and manufacturers) involved in its supply chain.

iii. The degree of any foreign ownership in or control of the entities identified under (i) and (ii) above.

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

v. Whether the Award Recipient and contractors (including but not limited to suppliers, distributors, and manufacturers), maintain a formal security program that includes:
    1) Personnel security;
    2) Physical security program;
    3) Information Technology security program; and
    4) Supply chain risk management program.

vi. The name and locations of each facility where any information system, information technology hardware and/or software to be delivered under the Award was designed, manufactured, packaged,and stored prior to distribution.

vii. The means and method for delivering any information system, information technology hardware (including but not limited to storage subsystems including hardware for software defined subsystems, switches and directors, de-duplication appliances, and storage virtualization appliances) and/or software to be delivered under the Award, including the names of any entity responsible for transport or storage. This information should address whether the information system, information technology hardware and/or software will be direct shipped to Government.

viii. Whether the proposed information system, information technology hardware and/or software includes a service agreement required by the Award, and if so, the identity of the contractor/subcontractor(s) who will provide this follow-on service, and how the services will be delivered/deployed (e.g., via on-site service? Remotely via internet?).

ix. The identity of the entity that will provide disposal services of any information system, information technology hardware and/or software required by the Award.

8. Cyber incident reporting requirement.

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

i. Conduct a review for evidence of compromise of covered Government information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered information system(s) that were part of the cyber incident, as well as other information systems on the network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Recipient's ability to provide operationally critical support; and

ii. Rapidly report cyber incidents to CISA PO at https://www.cisa.gov/forms/report

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

9. Within a time mutually agreed upon by the Awardee and the cognizant Program Officer, the Recipient must provide a written Summary of the policies, procedures and practices employed by the Recipient as part of theAwardee's IT security program, in place or planned, to protect activities in support of the Award.

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

The Summary will be the basis of a dialogue which CISA PO will have with the Recipient, directly or through

meetings. Discussions will address a number of topics, such as, but not limited to, evolving security concerns and concomitant cyber-security policy and procedures within the Government and at the Recipient, available education and training activities in cybersecurity, and coordination activities.

E. CLASSIFIED SECURITY CONDITIONS

1. "Classified national security information," as defined in Executive Order (EO) 12958, as amended, means information that has been determined pursuant to EO 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

2. Recipient access to classified information is required under this Cooperative Agreement. Before access to classified information is allowed, a Facility Clearance will be attained and individuals accessing classified information will have eligibility determined through the personnel security process. The maximum level of classification is Top Secret/SCI. The details will be specified in a Department of Defense (DD) Form 254. Accordingly, specified DHS/CISA liaison/analyst employees provided for this requirement must be eligible for a Top Secret/SCI Clearance.

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

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

5. Where an 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 thecontractor, subrecipient- or other entity without prior written approval from the DHS Office of Security,Industrial Security Program Branch (ISPB), or, an appropriate official within the Federal department or agency with whom the classified effort will be performed.

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

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

DHS Office of Security ISPB contact information:
Telephone: 202-447-5346
Email: IndustrialSecurityTeam@hq.dhs.gov

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

8. Sensitive Compartmented Information:

a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).

b. SCI will not be released to Recipient employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated Recipient.

c. All Recipient personnel requiring access to SCI as part of this Award effort must be approved and indoctrinated by CISA. Requests for Access will be submitted by the government project manager who can validate the justification for access.

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

e. SCI furnished in support of this cooperative agreement remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the Award, SCI furnished will be returned to the direct custody of the supporting SSO or destroyed in accordance with instructions outlined by the Grants Officer.

f. Visits by Recipient Personnel will only be certified by CISA when such visits are conducted as part of the cooperative agreement effort.

g. No SCI activities will occur at the Recipient location until the facility has been accredited by DHS or a co-utilization agreement is made between DHS and the current facility Government accrediting authority. DHS accreditation of an SCI Facility must be requested via the DHS Office of Security of Determination Authority and Cognizant Security Authority at SKIFAccreditation@hq.dhs.gov. The request for accreditation will include a concept of operations (CONOPS) which describes the operational requirement, facility description, and security oversight. Upon approval of the CONOPS, a fixed facility checklist and Standard Operating Procedures will be submitted for review and approval. Co-utilization agreement will be requested by the Recipient to the current accrediting authority and coordinated with DHS/OCSO. A copy of the approved co-utilization agreement will be provided to DHS/OCSO/SSPD prior to SCI activities occurring at the Recipient location.

h. DHS will inspect all SCI Facilities accredited by DHS, security policies and procedures, and all material generated or processed under the purview of this cooperative agreement:

i. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security offices (SSO).

ii. SCI will not be released to Recipient employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated Recipient.

iii. All Recipient personnel requiring access to SCI as part of this cooperative agreement must beapproved and indoctrinated by CISA. Requests for Access will be submitted by the government project manager who can validate the justification for access.

iv. Inquiries pertaining to classification guidance on SCI will be directed to the SSO.

v. SCI furnished in support of this cooperative agreement remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the cooperative agreement, SCI furnished will be returned to the direct custody of the supporting SSO or destroyed in accordance with instructions outlined by the Grants Officer.

vi. Visits by Recipient employees will only be certified by CISA PO when such visits are conducted as part of the cooperative agreement effort.

vii. SCI will be stored and maintained only in properly accredited facilities at the Recipient location.

viii. All Recipient requests to process SCI electronically will be sent to the accrediting SSO for coordination through appropriate SCI channels.

F. CONTROLLED UNCLASSIFIED INFORMATION

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

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

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

b. Ensure that all CISA CUI is protected by a physical or electronic barrier when not under direct individual control of an authorized user and limit the transfer or CISA CUI to subcontractors or teaming partners with a need to know and commitment to this level of protection.

c. Ensure that CISA CUI on mobile computing devices is identified and encrypted, and all communications on mobile devices or through wireless connections are protected and encrypted.

d. Overwrite media that has been used to process CISA CUI before external release or disposal.

e. The parties understand that information and materials provided pursuant to or resulting from this Award may be export controlled, sensitive, for official use only, or otherwise protected by law, executive order, or regulation. The Recipient is responsible for compliance with all applicable laws and regulations. Nothing in this Award shall be construed to permit any disclosure in violation of those restrictions.

G. HANDLING OF INFORMATION

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

1. Within the methodology and protocols defined above, Recipient or its agents will ensure that only its personnel, members, or agents approved by CISA PO who will be directly involved in managing and securing information systems will have access to unclassified, but Sensitive Federal Government information and analytical products.

2. Recipient shall adhere to any dissemination control markings clearly displayed on written documents containing any cybersecurity information shared under this Agreement.

3. Prior to sharing with the Federal Government, Recipient will remove information not directly related to a Cybersecurity Threat the Recipient knows at the time of sharing to be personal information of a specific person.

4. Recipient will ensure that any risk mitigation efforts, including use of Defensive Measures, that are based on government provided information, do not initiate communications with related threat resources defined within government provided information unless the Recipient is acting upon information obtained from other sources or transactions.

5. If Recipient uses government-provided information to enhance cyber threat detection and/or prevention services to third parties not covered by this Award, Recipient must notify CISA of any possible cyber threats detected and/or prevented using this information, as well as the name of each associated third-party entity.

6. With respect to CISA and other federal government provided information that the Recipient disseminates to non-federal entities when carrying out the scope of work under this Award, such information will remain the property of the federal government and is not releasable by the non-federal entities without express CISA authorization. Recipient will communicate that fact to such non-federal entities in order to ensure that, if a state, local, tribal, or territorial (SLTT) government receives a freedom of information or similar request under state, local, or tribal law, that SLTT government is able to appropriately process that request in light of the federal government's ownership of such information and prohibition against releasing that information without express CISA authorization.

H. NOTICE AND CONSENT CERTIFICATIONS

1. Recipient must comply with the U.S. Constitution, including the Fourth Amendment, any similar provisions in

State Constitutions, and relevant Federal and State-level electronic communications and privacy statutes.

2. Recipient provides security services (including enhanced netflow/IPFIX, intrusion detection and intrusion prevention, endpoint detection and response (EDR)), to State, local, tribal, and territorial governments, and their individual agencies (Recipient Customers). Before providing managed security services including enhanced netflow/IPFIX, intrusion detection, intrusion prevention, endpoint detection and response, or any other services that potentially acquire the content of electronic communications or data stored on, transiting, or being processed by a network or device, such as Cybersecurity Incident Response Support as described in Appendix A section 4.2.2.1, Recipient will obtain signed certifications substantially similar to the below from each new Recipient Customer. Recipient must obtain multiple certifications from Recipient Customer sub-entities as necessary to ensure that all users for whom such data will potentially be collected are covered by a certification. The certifications must state that Recipient Customer's computer users have received notice and consented to the following:

    a. Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Recipient Customer's information system; and

    b. All communications and data transiting or stored on or traveling to or from the Recipient Customer's information system will be monitored and may be disclosed or used for any lawful government purpose.

3. In the event that certain Recipient Customers request to sign a different form of certification or otherwise request an exception to the requirements in this paragraph, Recipient shall receive CISA approval to modify the requirements of this paragraph. Recipient's point of contact for such requests is OCC_Cyber@cisa.dhs.gov.

4. Recipient will provide the certifications described above to CISA upon CISA PO request.

I. COMPLIANCE WITH U.S. EXPORT CONTROLS

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

All documentation, as well as any questions or concerns regarding export controls, should be submitted to the RCO at exportcontrols@hq.DHS/CISA.gov.

J. PATENT RIGHTS, DATA RIGHTS, AND TRADEMARKS

1. PATENT RIGHTS

The Recipient is subject to applicable regulations governing patents and inventions, including government- wide regulations issued by the Department of Commerce at 37 C.F.R. Part 401, "Rights to Inventions Made by

Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements." The standard patents clause at 37 C.F.R. § 401.14 is incorporated by reference. All reports of subject inventions made under this Award should be submitted to CISA using the Interagency Edison system website at https://www.iedison.gov/ .

2. INTELLECTUAL PROPERTY EVALUATION CRITERION (or sub-criterion).
The operation and maintenance of software p, and any new software acquired under the Award or developed during the Period of Performance of this Award must:

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

   b. be capable of being seamlessly handed over to a successor Recipient or contractor skilled in the art of computer programming, maintenance, and upgrading, including documentation and licensing of any third-party software components or modules; and,

   c. assure that the ability of the software is contemporaneously archived to assure stability and the ability to survive outages.

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

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

4. DATA RIGHTS
CISA has the right to:

   a. Obtain, reproduce, publish, or otherwise use the data produced under the Award; and

   b. Authorize others to receive, reproduce, publish, or otherwise use such data for Federal purposes

   Data produced under the Award includes, but is not limited to, software.

K. COMPUTER SOFTWARE

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

a.

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

to do so.

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

    a. Commercial or Proprietary Software Components: Software, especially computer software used for online products and services, must be commercially available off-the-shelf, unless the CISA PO authorizes otherwise. The Recipient may not incorporate into the computer software content that is subject to either commercial or proprietary license conditions without the prior approval of the CISA PO.

    b. Computer Language: The Recipient must design and produce the software using the languages and specifications as directed by the CISA PO.

    c. Open-Source Software Components: To the extent that the Recipient intends to incorporate open-source content into the computer software, it may use open-source content subject to an open-source license that either requires only acknowledgement of the source or the source and a disclaimer of liability. Prior to incorporating open-source content subject to any other license conditions, the Recipient must request and receive the prior written approval of the CISA PO.

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

    a. Operable Source Code: The Recipient must deliver at the conclusion of Award performance one computer disc or make downloadable electronically as directed by the DHS Grants Officer, software containing the complete, easy to compile, and operable source code in the CISA approved language.

    b. Executable Code: The Recipient must deliver at the conclusion of Award performance one computer disc or make downloadable electronically as directed by the DHS Grants Officer, software containing the complete and operable executable code.

    c. Software Documentation: The Recipient must create and deliver software documentation that contain programmer notes describing the following:

        i. The software's operation, organization, and any significant characteristics of its design.

        ii. The foregoing information provided such that a computer programmer skilled in the art of programming according to the approved language may operate, maintain, update, modify, and perform all operations necessary to perpetuate the utility of the computer software.

    d. Description of Third-Party Licenses Used. To the extent that the Recipient has included in the computer software, either CISA approved open-source content or software content subject to proprietary licenses, the Recipient must provide each of those licenses and incorporate those licenses in a delivered file.

5. Independence of Cloud Based Software: The Recipient must rely on high-performance computing resources. A key measure of innovation is leveraging the capabilities of cloud computing for analytics, collaboration, and workflow with non-Recipients. The Recipient must ensure that cloud computing software is capable of running on non-Recipient based systems. Any cloud-based software must be capable of running on equivalent CISA or third-party servers. This attribute must be an aspect of the software's underlying design.

6. Interoperability of Related Data: Data derived from the created software must be capable of being transferred to other software in a machine legible format with a minimal level of outside intervention when consistent with standard industry practice. This attribute must be part of the software's underlying design.

7. Testing of Software.

    a. Software Testing Required. Any software created under interagency agreement, contract, other transaction agreement, or cooperative agreement prior to delivery must undergo software testing. Software testing must be conducted using industry standard tools and in the testing environments identified in the Recipient's proposal under the heading titled "Program Management Plan Major Milestone(s)", incorporated herein by reference.

    b. Timing of Software Testing. Software testing should occur once executable software has been created.

    c. Software Testing Requirements. Software testing should determine the following:
        i. That the software can serve the purpose of its creation and meets the requirements.

        ii. That the software is stable and performs correctly to all inputted information.

        iii. The software is usable and performs its functions within a time frame appropriate for the nature of the operation.

    d. Installation Testing. Installation testing that identifies what will be necessary for a user to install and successfully run the software will be required prior to delivery.

L. PUBLICATIONS

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

> Acknowledgement. "This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, (xxxxxxxxxx)."
> Disclaimer. "The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security."

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

2. Enhancing Public Access to Publications. The Recipient may copyright any work that is subject to copyright and was developed, or for which ownership was acquired, under this Award. CISA reserves a

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

3. Coordination of Public Statements

a. Any public references to or descriptions of the program activities undertaken under this Agreement by the Recipient, or any Analytical Products produced jointly by the Recipient and CISA PO under this Agreement will be done only after coordination, in writing between the Recipient and CISA PO.

b. The Recipient must notify the CISA PO of public or media events publicizing the accomplishment of significant events as a result of this agreement and provide the opportunity for attendance and participation by federal representatives with at least ten (10) working days' notice.

M. SITE VISITS

CISA PO, through authorized representatives, has the right, at all reasonable times, to make site visits to review project accomplishments and management control systems and to provide such technical assistance as may be required. If any site visit is made by CISA PO on the premises of the Recipient, or a contractor under this Award, the Recipient must provide and must require its contractors to provide all reasonable facilities and assistance for the safety and convenience of the Government representatives in the performance of their duties. All site visits and evaluations will be performed in such a manner that will not unduly delay the work.

N. TRAVEL

Travel required in the performance of the duties approved in this Award must comply with 2 C.F.R. § 200.474. **Foreign travel must be approved by CISA PO in advance and in writing.** Requests for foreign travel identifying the traveler, the purpose, the destination, and the estimated travel costs must be submitted to the DHS Grants Officer 60 days prior to the commencement of travel.

O. PUBLIC HEALTH

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

P. TERMINATION

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

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

Q. GOVERNING PROVISIONS

The following are incorporated into this Award by reference:

31 C.F.R. Part 205	Rules and Procedures for Funds Transfers
2 C.F.R. Part 200	Uniform Administrative Requirement, Cost Principles, and Audit Requirements for Federal Awards
NOFO	DHS-23-CISA-123-ISAC000001
Application	Grant Application and Assurances dated September 2023

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.