The Department of Homeland Security (DHS)
Notice of Funding Opportunity (NOFO)
State, Local, Tribal and Territorial Indicators of Compromise Automation Pilot

NOTE: If you are going to apply for this funding opportunity and have not obtained a Data Universal Numbering System (DUNS) number and/or are not currently registered in the System for Award Management (SAM), please take immediate action to obtain a DUNS Number, if applicable, and then to register immediately in SAM. It may take 4 weeks or more after you submit your SAM registration before your registration is active in SAM, then an additional 24 hours for Grants.gov to recognize your information. Information on obtaining a DUNS number and registering in SAM is available from Grants.gov at: http://www.grants.gov/web/grants/register.html Detailed information regarding DUNS and SAM is also provided in Section D of this NOFO, subsection, Content and Form of Application Submission.

A. Program Description

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

Assistance Listings Number (formerly Catalog of Federal Domestic Assistance Number)
97.128

Assistance Listing Title (formerly CFDA Title)
State, Local, Tribal and Territorial (SLTT) Indicators of Compromise Automation

Notice of Funding Opportunity Title
State, Local, Tribal and Territorial (SLTT) Indicators of Compromise – Automation Pilot

NOFO Number
DHS–19-CISA-128-SLT001

Authorizing Authority for Program
Homeland Security Act of 2002, as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018, National Cybersecurity Protection Act of 2014, Executive Order (EO) 13636, Executive Order 13691, Presidential Policy Directive (PPD) 21

Appropriation Authority for Program
Department of Homeland Security (DHS) Appropriations Act, 2019, P.L. 116-6, Title III, Cybersecurity and Infrastructure Security Agency

Program Type
New Cooperative Agreement

Program Overview, Objectives, and Priorities
The Cybersecurity and Infrastructure Security Agency, Cybersecurity Division, Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) seeks to award a new cooperative agreement for a pilot titled "State, Local, Tribal and Territorial (SLTT) Indicators of Compromise – Automation Pilot in fiscal year 2019. This agreement supports implementation of the Homeland Security Act of 2002, as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018, Subtitle A, SEC. 2209, specifically with respect to facilitating information sharing related to cybersecurity risks, incidents, analysis, and warnings, and providing technical assistance.

Justification: the nature of the cybersecurity threat to America is growing, and our nation's cyber adversaries move with speed and stealth. To keep pace, all types of organizations, including those beyond traditional critical infrastructure sectors, need to be able to share information and respond to cyber risk in as close to real-time as possible. Organizations engaged in information sharing and responding to indicators of compromise in "real-time" play an invaluable role in the collective cybersecurity of the United States.

The purpose of this cooperative agreement is to apply the usage of automation to enhance and speed the evaluation of threat Indicators of Compromise (IOC) at the state and local government levels. In addition, the pilot will identify key areas for potential reduction of manual tasks by humans and actionable information sharing across enterprises and SLTT. The pilot will also identify orchestration services needed to integrate the activities of sensing, understanding, decision-making, and acting. The grant recipient may select up to five states and/or localities to participate in the pilot project. The pilot project will focus on developing model processes, methods, and accompanying policies and procedures that can be applied by SLTT to accomplish the following:

- Action upon IOCs within minutes of receipt.
- Reduce time spent on repetitive tasks.
- Provide generation, enrichment and scoring of IOCs.
- Receipt, remediation and response to IOCs.
- Demonstrate the use of Security Orchestration, Automation, and Response (SOAR) operational procedures and capabilities combined with information sharing to make data more actionable and enable consistent execution at and across SLTT levels.
- Development of repeatable processes for orchestration and automation services that bridge existing SLTT policies with SOAR capabilities.

To fulfill this requirement DHS will select an organization through an open and competitive process and enter into a cooperative agreement.

The grants officer will oversee the execution of the grant and the performance of grant execution based on input from the DHS, CISA, CSD Program Office, discussion with the awardee, and Program Performance Reporting Requirements (found in Section F and Appendix A).

Security Automation an Orchestration (SA&O) Operational Performance measures and metrics

Quarterly Performance Metrics must be submitted to the DHS Grants Officer no later than 30 days after the end of each quarter. Reports are due October 30, January 31, April 30 and July 31**.** Reports shall be submitted via the GrantSolutions **Grant Note** feature using the **Grant Note submission guidance** found here: https://www.grantsolutions.gov/support/granteeUsers.html.

SA&O metrics and measures assist organizations in recognizing and refining how SA&O capabilities and techniques introduce benefits, value and effects. This document identifies metrics and measures that organizations may find beneficial to collect, assess, and compare over time.

Metrics and Measures Groupings
1. **Operational Performance - evaluate & recognize SA&O value, benefits, issues and effects as it relates to security operations and performance.** 2. **System Performance - evaluate & recognize value, issues and effects as it relates to your Cyber security infrastructure, practices and SA&O support.** 3. **Process Performance – evaluate & recognize value, issues, and effects as it relates to organizational, practice and process dependencies that directly impact SA&O value.** 4. **Workflow Execution - assist organizations to design, develop, monitor, tune, troubleshoot and maintain SA&O capabilities.** ** The groupings are general to highlight types of metrics and measures and are not comprehensive*

As organizations apply SA&O capabilities, there is value in collecting information to help assess utility, applicability, (in) efficiency, and reliability of the implementations. It is also useful to collect information that identifies dependencies, opportunities for improvements, or changes in performance. Lastly, it may be important to collect audit information to support deployment testing or compliance verification.

Metrics and Measures may be tailored for performance indicators as:

- Quantitative – measure of value (number, time, $, ratio)
- Qualitative – measure of acceptability or health
- Thresholds – when an index reaches set targets or falls into set ranges
- Milestones – when a specific condition is reached
- Trends – results analyzed over time and volume

Metrics and Measures

The following tables provide insight into metrics and measures that can be captured or produced by SA&O systems. Each entry includes a description and rationale/utility examples.

SA&O Operational Performance measures and metrics

Assist organizations to evaluate and recognize SA&O value, benefits, issues and effects. They offer insights for how SA&O has been applied, efficiencies gained, cyber security operations effectiveness and overall Return on Investment (ROI) context. Because they are directly related to reasons that organizations invest in SA&O, most of these metrics and measures are already "provided" by orchestration providers and described in industry resources.

Measure/Metric	**Description**	**Rationale/Utility** *Identifies or Informs*
Operational Performance		
1. Mean time to notification	Time between a potential malicious activity detected and an alert is provided to the person or system responsible for investigating.	• Summarize operational value when compared with prior practices • Example: Time lapse notifying SOC tier 1 support
2. Mean time to investigation	Once an alert has been sent, how much time passes before the investigation begins and what is the duration of the investigation?	• Throughput • Summarize operational value • Ability to handle higher volumes of investigations, alerts and data • Example: Time lapse between notification and when an automated workflow or analyst begins investigating
3. Mean time to remediation	From alert to investigation to remediation, total elapsed time.	• Summarize operational value • If organization achieving quicker detection and response • Example: Average time to resolve a number of major vs. minor incidents
4. Remediation summary statistics	Statistics tracking manual, semi- automated and automated remediation	• Characterize the level of automation applied in operations • Track progression for each type of remediation • Summarize operational value • Example: Summarize the types of incidents aided by workflows for remediation
5. Percent Investigated vs. Alert Volume	Investigations vs. alert volume	• Security Operations risk gap • How SA&O aids investigations compared to the volume of alert data

6. Performance Improvements	Information collected to show how automation is improving processes and resource utilization.	• Operational value in terms of performance • Resource savings • Examples: speed of decision/resolution, resource utilization improvement (e.g., devices run faster due to less malware, increased network bandwidth due to blocking malware related traffic)

System Performance measures and metrics

Assist organizations to evaluate & recognize value, issues and effects as it relates to your cyber security infrastructure, practices and SA&O support. They offer insights for how SA&O has been implemented, orchestration management, and cyber security product/service value as related to automation in operations.

Measure/Metric	Description	Rationale/Utility *Identifies or Informs*
System Performance and Utilization		
7. Workflow utility	Track how many incidents and types of incidents were aided by workflows.	• Utilization trends • Operational value for incident and alert triage • Operational practices and dependencies • Example: Identify if workflows are or could address common incidents/alerts in part or whole.
8. Sensor utilization	Track playbook/workflow dependencies on sensors, threat feeds and data sources.	• Potential impact of compromised or unavailable sensor(s) • Heavily vs. underutilized sensor(s) • Which sensors aid investigation and/or remediation actions • Example: Which workflows rely on real- time packet capture analysis? Impact if it were to become unavailable?

9. Sensor value	Track which sensors, threat feeds and data (sources) aided an investigation or remediation	• Potential impact of compromised or unavailable sensor(s) • High valued vs. underutilized sensor(s) • Sensor tuning effectiveness • Which sensors aid investigation and/or remediation actions • Example: Types of logs or threat feeds and indicators proven effective
10. Threat Indicator or IOC value	Track which threat indicator(s) aided an investigation or remediation	• Types and sources of indicators aiding security operations
11. Queued workflows or actions	Number of playbooks, workflows, investigations queued	• Ability to scale and support demand • Identify system bottlenecks • Throughput • System failures • Examples: Understanding if the system is capable of supporting operational demand
12. Concurrency/ Parallel workflows	Number of playbooks, workflows or investigations executed per time period	• Ability to scale and support demand • Examples: Comparing workflow executions with Incident triage in peak time periods
13. Workflow interface dependencies	Track which product integration interfaces were used in or are required for workflow execution	• Security infrastructure dependencies • Common, duplicative vs. purposely separated system interfaces • Example: Common dependency on a logging interface and impact if it were to become compromised or unavailable.
14. Performance Degradation	Information collected to show how automated processes are negatively impacting system or process performance.	• Counterproductive operational impact • Example: boundary protection devices run slower due to increasingly large blacklists or decreased network bandwidth due to queries to support internal enrichment of IOCs

15. Custom Measures & Metrics	Enable admins and users to create and save measures or calculations for use in analysis	• Performance measures and Key Performance Indicators differ by organization, culture and goals. Offer the flexibility for organizations to define and analyze performance and results. • Examples: unauthorized software/devices identified in investigations, percentage of devices with current patches, detected non- compliance with business conduct policies, and number of reported vs. detected security incidents

Process Performance measures and metrics

Assist organizations to evaluate & recognize value, issues, and effects as it relates to organizational, practice and process dependencies that directly impact SA&O value. They offer insights for how SA&O efficiency and effectiveness may be impacted by dependencies on external, manual, poorly-defined, and/or cross-organizational processes.

Measure/Metric	**Description**	**Rationale/Utility** *Identifies or Informs*
Process Performance		
16. External process dependencies	Identifies workflows that have a dependency on an external process or system	• Operational dependencies across organizations, systems, tools and practitioners Examples: Third party service or cloud providers, inter-organizational relationships NOC/SOC/IT
17. Workflows requiring human intervention (as designed)	Track playbook/workflow dependencies on human interaction	• Workflows that require an approval or human interaction as part of execution • Workflows that can execute without human interaction • Classifying how different types of workflows may benefit by manual or automated validation, verification and/or audit. • Example: Identify frequently executed workflows with a history of high confidence execution still requiring human interaction.

18. Workflow effectiveness	Track which workflows were effective for their intended goal vs. required additional investigation or analysis.	• Poorly defined processes that cannot be automated consistently • Opportunities to enhance workflows and reduce manual processing required • Additional sensors, sources and/or analysis techniques relevant to the task • Example: Percentage or number of investigations and workflows which required unanticipated analyst investigation support.
19. Analyst/ Practitioner/ Organization interactions	Track which organizations and staff were required to interact with a workflow to facilitate an end goal. Track within and across connected workflows	• Organizational dependencies • Opportunities to streamline operations across organizations • Inform service level agreements between organizations • Examples: SOC, NOC, IT, Helpdesk, and Legal

Workflow Execution measures and metrics

Assist organizations in verifying that SA&O performance is achieving intended effects. As part of that, these metrics and measures assist organizations in the design, development, monitoring/auditing, tuning, troubleshooting, and maintenance of SA&O capabilities.

Measure/Metric	**Description**	**Rationale/Utility** *Identifies or Informs*
Workflow Execution		
20. Frequency of workflow revisions	Statistics tracking the frequency of workflow/playbook revisions	• Stability of workflows • Complexity of workflows • Controlled administration, configuration & tuning • Audit authorized & verified changes • Automated tests to verify and validate results and intent. • Example: Stable workflows suddenly revised or unapproved changes to operational practices.

21. Frequency of workflow execution	Statistics tracking the frequency of workflow/playbook execution	• Potential impact to operations if compromised or unavailable • Frequency of initiating condition or alerts • Example: Identify how often the workflow executes during business hours
22. Frequency of remediation actions taken	Statistics tracking the frequency of actions taken to remediate threats/risks	• Audit changes made to operational assets • Frequency of changes made to certain operational assets • Example: Identify how often the workflow executes different actions in response to same trigger
23. Workflow utilization	Track how many times a workflow is selected manually vs. automated and runs.	• Utilization trends (heavily vs. underutilized) • Operational practices and dependencies • Example: Identify if and how analysts and/or automated responses are applying workflows.
24. Workflow value	Savings estimate by multiplying the cost of performing repetitive tasks manually by the estimated number of times the system performs those tasks automatically during a specific date/time range.	• Estimated time and/or cost savings • Return on Investment (ROI)
25. Workflow confidence level	Statistics tracking the frequency automated recommendations are confirmed for execution	• Confidence in semi-automated/automated COA recommendations • Potential workflows to enhance with automation • Example: Workflow confidence score increases given the frequency analysts concur with recommendations.
26. Workflow idle time	Statistics tracking times workflows were paused waiting for data, a decision, action or approval.	• Efficiency opportunities for processes and workflows • Throughput/efficiency constraints • Sources of bottlenecks • Example: SOC workflow commonly requires network operations center (NOC) concurrence which is taking 24-48hrs. Opportunity to accelerate between departments?

27. Workflow reliability	Track successful vs. unsuccessful executions. (success, failure, error rates)	• Reliability trends • Failures common across workflows • Example: Workflow A is highly reliable while workflow B commonly requires unplanned manual intervention and should be considered for revision.
28. Workflow decision processing	Capture triggering condition, key values/decision points, and end state	• Verify that certain actions are taken if and only if certain conditions are true. • Example: provide evidence that a critical server is not taken offline and reset unless another service is verified as online first.
29. Workflow dwell time	Statistics tracking workflow execution times	• Performance (typical vs. abnormal) • Change in system or capabilities • Example: A workflow typically requires 1 minute to complete and is noted taking 2+ mins. Intended or unintended change?
30. Workflow deployment readiness	Evidence verifying and validating workflows are defined by compliant practices and execute as intended.	• Workflow dependencies • If workflows can be verified, audited and validated • Examples: verification that initiating feeds are working, timing information on how long certain paths or steps take, responses from sensors or actuators tasked

B. Federal Award Information

Award Amounts, Important Dates, and Extensions

Available Funding for the NOFO: $2,000,000.00.

Projected number of Awards *(Optional)*: 1 (one) award.

Period of Performance: 12 months.

Extensions to the Performance Period may be awarded but are not guaranteed. Extension approvals will be based on the availability of funds within the award and acceptable performance.

Projected Period of Performance Start Date(s): 10/1/2019

Projected Period of Performance End Date(s): 09/30/2020

Funding Instrument: Discretionary – Competitive – Cooperative Agreement

DHS will exercise substantial programmatic involvement through this cooperative agreement. This includes conducting site visits and quarterly monitoring of project progress; providing technical assistance; overseeing agency review and approval required at the completion of one stage of the work prior to moving on to subsequent phases; reviewing and approving of sub-grants that exceed standard regulatory approvals; work plans or modifications thereto; holding kickoff meetings; conducting bi-annual programmatic reviews; coordinating standards development and self-certification activities.

The grants officer will oversee the execution of the grant and the overall performance of the awardee from an administrative and financial perspective.

C. Eligibility Information

Eligible Applicants

- For-profit organizations other than small businesses
- Nonprofits with 501(c) (3) IRS status, other than institution of higher education
- Nonprofits without 501(c) (3) IRS status, other than institution of higher education
- Federally Funded Research and Development Centers (FFRDCs)
- University Affiliated Research Centers (UARCs)
- Private institutions of higher education
- Public and State controlled institutions of higher education
- Small businesses

Eligibility Criteria

To be eligible for this program, must meet the below requirements.

1. Applicants must not be a Government organization. Pursuant to EO 13691, "Promoting Private Sector Cybersecurity Information Sharing" of February 13, 2015, the organization selected must be non-governmental to be eligible. DHS has interpreted this restriction to exclude federal, state, local, territorial, tribal, and foreign governmental entities from making a proposal for this announcement.
2. At the time of application, applicants must have at least three years of experience developing cybersecurity best practices for SLTT Governments.
3. Applicants must have qualified and experienced to gather, analyze, and disseminate government and critical infrastructure information that can be shared at machine speed across SLTT. Recent and extensive experience providing cybersecurity-related information sharing, interoperability and automation best practices development.
4. Applicants must have at least three years of experience coordinating engagements with SLTT, private companies, Federal agencies, and subject matter experts engaged in

addressing advances in orchestration and automation services for improved interoperability, information sharing and automation of network defenses.

5. Applicants must have three years of experience conducting research and analysis on the most effective methods for advancing cybersecurity, IOC automation, and demonstrating the usage and effectiveness of SOAR capabilities.
6. Applicants must have deep knowledge of the National Infrastructure Protection Plan, Executive Order 13636, Executive Order 13691, and PPD-21.
7. Federal agencies may not apply. Federal employees are not eligible to serve in a principal leadership role on a grant or cooperative agreement, and may not receive salaries or in other ways augment their agency's appropriations through awards made by this program.

    a. Nonetheless, federal employees may interact substantively with awardees in the form of cooperation.
    b. Cooperation involves consulting on the planning, management, and coordination of standards organization and/or information sharing and analysis organization activities, sharing or comparing information, indicators, samples, equipment, facilities, data, models, or other support during the conduct of the standards development and related activities in which the interaction is substantial and requires the award of a cooperative agreement, rather than a grant.
    c. Substantial involvement occurs when the collaboration or cooperation of a federal employee or facility is necessary to achieving the overall goals of the activities supported by this cooperative agreement.

Other Eligibility Criteria

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

1. **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.
2. **Application relevance.** Applications that do not address the purpose of this announcement will not be considered.
3. **Compliance and completeness.** Applications must substantially comply with the application submission instructions and requirements in this announcement or they will not be considered.
4. **Funding limits.** Applications exceeding the funding limits will not be considered.
5. **Proof of non-profit status.** Non-profit applicants and any proposed sub-awardee of a non-profit must provide documentation of non-profit and/or public status. This requirement does not apply to for-profit applicants. Any of the following constitutes acceptable proof of non-profit status:

- 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.
- A copy of a currently valid IRS tax exemption certificate.
- 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.
- A certified copy of the organization's certificate of incorporation or similar document that clearly establishes non-profit status.
- 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.
- A signed statement on official letterhead by an official authorized to apply for grant funds on behalf of the public entity shall suffice.

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.

Maintenance of Effort (MOE)
There is no maintenance of effort requirement for this program. Requests for funds under this announcement shall not be used to take the place of activities described in the application that are currently supported with other funding. Also, grant funds shall not be used to support activities that are a normal part of the organization's operations.

Cost Share or Match
There is no cost share or match requirement for this program.

D. Application and Submission Information

Key Dates and Times

Date Posted to Grants.gov: 08/12/2019

Application Submission Deadline: 08/28/2019 at 11:59:59 /PM [EDT]

Anticipated Funding Selection Date: 09/10/2019

Anticipated Award Date: 09/25/2019

Address to Request Application Package

Application forms and instructions are available at Grants.gov. To access these materials, go to http://www.grants.gov , select "Applicants" then "Apply for Grants." In order to obtain the application package select "Download a Grant Application Package." Enter the CFDA and/or the funding opportunity number located on the cover of this NOFO, select "Download Package," and then follow the prompts to download the application package.

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

Stephanie Dawkins
Grants Officer
stephanie.dawkins@hq.dhs.gov
Phone: 202-447-0495

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. If you experience difficulties accessing information or have any questions, please call Grants.gov customer support at 1-800-518-4726.

Hard copy applications will not be accepted.

Content and Form of Application Submission
Applicants must submit all required forms and required documents listed in this section. See the Grants.gov Applicant User Guide for instructions on how to attach forms and documents. Applicant should ensure that the final submitted application package includes all required forms and documents. Applicants should avoid the use of special characters in attachment file names.

Unique Entity Identifier and System for Award Management (SAM)
All applicants for this award must:

1. Be registered in SAM before submitting its application;
2. Provide a valid DUNS number in its application; and
3. Continue to maintain an active SAM registration with current information at all times during which it has an active federal award or an application or plan under consideration by a DHS FAO.

DHS may not make a federal award to an applicant until the applicant has complied with all applicable DUNS and SAM requirements and, if an applicant has not fully complied with the requirements by the time DHS is ready to make a federal 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.

The Standard Language for Using Grants.gov Apply is provided to aid in fulfilling these requirements:

Electronic Delivery

DHS is participating in the Grants.gov initiative to provide the grant community with a single site to find and apply for grant funding opportunities. DHS encourages applicants to submit their applications online through Grants.gov.

How to Register to Apply through Grants.gov

1. *Instructions:* 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 Data Universal Numbering System (DUNS) Number, active System for Award Management (SAM) registration, and Grants.gov account to apply for grants.

   If individual applicants are eligible to apply for this grant funding opportunity, refer to: https://www.grants.gov/web/grants/applicants/registration.html

   Organization applicants can find complete instructions here: https://www.grants.gov/web/grants/applicants/organization-registration.html

2. *Obtain a DUNS Number*: All entities applying for funding, including renewal funding, must have a Data Universal Numbering System (DUNS) number from Dun & Bradstreet (D&B). Applicants must enter the DUNS number in the data entry field labeled "Organizational DUNS" on the SF-424 Form.

   For more detailed instructions for obtaining a DUNS number, refer to: https://www.grants.gov/web/grants/applicants/organization-registration/step-1-obtain-duns-number.html

3. *Register with SAM*: In addition to having a DUNS number, 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.

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

4. *Create a Grants.gov Account*: The next step in the registration process is to create an account with Grants.gov. Applicants must know their organization's DUNS number to complete this process.

   For more information, follow the on-screen instructions or refer to: https://www.grants.gov/web/grants/applicants/registration.html

5. *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 of your grant applications. To add an organizational profile to your Grants.gov account, enter the DUNS Number for the organization in the DUNS 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

6. *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 is 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

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

8. *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 individuals who are able to make legally binding commitments on behalf of the organization as an AOR; **this step is often missed and it is crucial for valid and timely submissions.**

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 grant team may simultaneously access and edit different

webforms within an application. For each funding opportunity announcement (FOA), 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

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

2. *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.

3. *Adobe Reader*: If you decide not to apply by filling out webforms you can download individual PDF forms in Workspace so that they will appear similar to other Standard or DHS forms. 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

4. *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.

5. *Complete SF-424 Fields First*: The forms are designed to fill in common required fields across other forms, such as the applicant name, address, and DUNS 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.

6. *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.

7. *Track a Workspace*: After successfully submitting a workspace package, 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 grant opportunity, contact the number listed in the application package of the grant you are applying for.

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

Timely Receipt Requirements and Proof of Timely Submission

Online Submissions. All applications must be received by **Midnight Eastern Daylight Time** 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 (GRANTXXXXXXXX) 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 shall 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. 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.

Intergovernmental Review

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 (see *http://www.fws.gov/policy/library/rgeo12372.pdf)*. Name and addresses of the SPOCs are maintained at the Office of Management and Budget's home page at *http://www.whitehouse.gov/omb/grants_spoc* to ensure currency.

Funding Restrictions

Restrictions on Use of Award Funds

As well as any funding restrictions stated in the Budget Narrative section or any section within this document, the following are restrictions on use of award funds:

1. 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.

DHS substantial programmatic involvement and performance/progress reviews may result in funding restrictions in conjunction with initial and annual continuation awards.

Management and Administration (M&A) Costs.

M&A is allowable by the primary recipient, if applicable.

Indirect Facilities & Administrative (F&A) Costs.

Indirect Costs are allowable for the grantee and any proposed sub-awardee (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 §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 CFR Part 200.414.

Other Submission Requirements

To access application forms and instructions for this funding opportunity, go to Grants.gov click on the "Search Grants" tab. Enter the FOA Number located on the cover of this announcement. Click on the highlighted Funding Opportunity # that appears and then click on the various tabs to: read the Synopsis; review the Version History; read the Full Announcement; and, complete the Application Package. Please read the entire FOA Application Package carefully before preparing and submitting an application. Application must be submitted in electronic format only.

If you experience difficulties accessing information or have any questions please call the grants.gov customer support hotline at (800) 518-4726.

E. Application Review Information

Application Evaluation Criteria

Prior to making a federal award, the <DHS FAO> is required by 31 U.S.C. § 3321 note, 41 U.S.C. § 2313, and 2 C.F.R. § 200.205 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.

DHS will use the following criteria to evaluate applications deemed eligible and responsive. Applicants can receive up to 100 points.

1. **Capacity to provide leadership in the automation of Indicators of Compromise and to make the data relevant and actionable for network defense. (30 Points)**

   The extent to which the applicant demonstrates:

   a. Knowledge of the most effective methods to automate the evaluation of Indicators of Compromise. (10 points).

b. Background with cybersecurity-related information sharing and the automating the evaluation of Indicators of Compromise, conducted pilots demonstrating that it is possible to define a process that optimizes time to mitigation by utilizing Security Automation and Orchestration technologies. (10 points).

c. Qualified and experienced to gather, analyze, and disseminate government and critical infrastructure cybersecurity information to SLTT. Recent and extensive experience providing cybersecurity-related information sharing and best practice development generally. (10 points).

2. Develop documentation including design, policies and procedures, CONOPS, and operations manual(s); (20 Points)

The extent to which the applicant demonstrates:

a. Develop policy and procedures from Information Sharing and Analysis Centers or Threat Intelligence Platforms to make data actionable, useable and consumable to SLTT. (20 points).

3. Capacity to Provide Wide Outreach to SLTT (40 Points)

The extent to which the applicant demonstrates:

a. Ability to deliver coordination engagements with SLTT and subject matter experts engaged in addressing cybersecurity automation use cases. (20 points)

b. Ability to coordinate and engage with SLTT agencies that own and operate critical infrastructure, to include but not limited to Election Infrastructure, to develop policies and procedures regarding IOC automation (20 Points)

4. Cost Effectiveness and Balance (10 Points)

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

Review and Selection Process

DHS 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. DHS will assemble reviewers which may include both federal and 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 DHS 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. DHS 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 grant award completion that includes the name of the grantor, amount awarded, and whether the grant recipient sufficiently completed the requirements of the grant award (e.g., a final close-out report, certification of grant award completion, etc.)
6. After the technical review and before making final funding decisions, DHS may contact the highest ranking applicants to seek clarification and to negotiate technical and programmatic aspects of the application. If an application includes a sub-awardee, DHS 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. DHS 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 DHS personnel.

   DHS screens all technical reviewers for potential conflicts of interest. To determine possible conflicts of interest, DHS requires potential reviewers to complete and sign conflicts of interest and nondisclosure forms. DHS will keep the names of submitting institutions and individuals as well as the substance of the applications confidential except to reviewers and DHS staff involved in the award process. DHS will destroy any unsuccessful applications after three years following the funding decision.

8 DHS 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 notice of funding opportunity.

9 DHS will notify all applicants electronically of funding decisions. Unfunded applicants may send a written request to the Grants Officer, stephanie.dawkins@hq.dhs.gov to receive a written summary of comments related to the evaluation criteria, along with the points awarded to the application for each of the evaluation criteria. DHS will send the written summary to the applicant within 60 days of the request. Additional information beyond that described here will not be provided.

Applications will be evaluated relative to the requirements of the funding opportunity announcement. Therefore, interested parties should be aware that evaluators will distinguish between what is required information and rationalizations, "brochuremanship," or extraneous information. Final consideration will, however, take into consideration additional information submitted that supports claims in proposals for this opportunity.

The Project Narrative evaluation will be conducted based on requirements outlined in Section A. of the funding opportunity announcement and set forth below. Section A provides the minimum requirements that the applicants must be able to meet for their applications to be considered responsive or acceptable.

The applicant has the responsibility to provide information that clearly demonstrates its ability to satisfactorily respond to the requirements of the funding opportunity announcement.

a. Project Participants. Evaluators will assess if qualified participants are included and assess the impact of any additional participants.

b. Need for Assistance. Evaluators will assess the application for thoroughness and completeness documenting the need for assistance, existing capabilities and coordination. Evaluators will focus on innovativeness of approach including ability to meet deliverables.

DHS has developed an Objective Review Plan (ORP). The Objective Review Plan Evaluators will assign ratings for each applicant. The ORP will then meet to develop a group consensus rating for the criteria listed in the NOFO.

The ORP Chairperson will be responsible for incorporating the evaluation into the ORP Report, based on the final consensus ratings assigned by the ORP.

The DHS approving official shall review and consider evaluations from departments and agencies to inform the selection process. However, the DHS approving official is not required to develop a consensus government-wide view or to adopt a majority view. No one single factor or

a single review is dispositive; rather, the totality of the information is to be considered by the approving official in his/her discretion.

NOTE: There is no cost share or match requirement for this program, therefore an applicant's proposed cost sharing will not be considered in the review process.

Supplemental Financial Integrity Review

If the anticipated federal share of a federal award will be greater than the simplified acquisition threshold, currently $250,000 (see Section 805 of the National Defense Authorization Act for Fiscal year 2008, Pub. L. No. 115-91, OMB Memorandum M-18-18 at https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-18.pdf):

i. Prior to making a federal award with a total amount of federal share greater than the simplified acquisition threshold, DHS is required to review and consider any information about the applicant that is in the designated integrity and performance system accessible through SAM (currently FAPIIS).

ii. An applicant, at its option, may review information in the designated integrity and performance systems accessible through SAM and comment on any information about itself that a federal awarding agency previously entered and is currently in the designated integrity and performance system accessible through SAM.

iii. DHS will consider any comments by the applicant, in addition to the other information in the designated integrity and performance system, 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. § 200.205 federal awarding agency review of risk posed by applicants.

F. Federal Award Administration Information

Notice of Award

DHS issues formal award notification documents following fulfillment of DHS Congressional notifications. All DHS grants and cooperative agreements are subject to the standard DHS Award Terms and Conditions, which are attached to this package.

A grant award will be executed by a DHS Grants Officer authorized to obligate DHS funding. Unsuccessful applicants will be contacted as well and will be encouraged to apply for future grant award programs. Announcements for future programs will be listed at http://www.grants.gov.

Administrative and National Policy Requirements

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

DHS Standard Terms and Conditions

The applicable DHS Standard Terms and Conditions will be for the last year specified at that URL, unless the application is for a continuation award. In that event, the terms and conditions in effect for the fiscal year that award was originally made will apply.

Before accepting the award, the AOR should carefully read the award package for instructions on administering the grant award and the terms and conditions associated with responsibilities under federal awards. Recipients must accept all conditions in this NOFO as well as any special terms and conditions in the Notice of Award to receive an award under this program.

Reporting

1. Quarterly Federal Financial Reports. The Recipient shall submit a Federal Financial Report (SF425) to the DHS Grants Officer no later than 30 days after the end of each quarter. Reports are due October 30, January 31, April 30, and July 31. The report shall be shall be submitted using the **FFR submission guidance** found here: https://www.grantsolutions.gov/support/granteeUsers.html

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

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

The Recipient shall be paid in advance using the U.S. Department of Health and Human Services/Payment Management System, provided it maintains or demonstrates the willingness and ability to maintain procedures to minimize the time elapsing between the transfer of the funds from the DHS and expenditure disbursement by the Recipient.

When these requirements are not met, the Recipient will be required to be on a reimbursement for costs incurred method.

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

Federal Financial Reporting Requirements.
The Federal Financial Reporting Form (FFR) is available online at:

SF-425 *OMB #4040-0014*

Program Performance Reporting Requirements

The recipient is required to submit the following performance reports:

1. Quarterly Performance Reports must be submitted to the DHS Grants Officer no later than 30 days after the end of each quarter. Reports are due October 30, January 31, April 30, and July 31. Reports shall be shall be submitted via the GrantSolutions ***Grant Notes*** using the **Grant Note submission guidance** found here: https://www.grantsolutions.gov/support/granteeUsers.html. Performance reports must provide information on the overall progress of the IOC Automation Pilot. These reports shall also include:

i. Summary reports on the strategic vision and activities; management efforts; performance reports on each funded project, along with explanations of any changes from the initially approved work plan, discussion of progress for each milestone and explanations of why milestones were not reached, the performance metrics used; budget expenditures and changes; unanticipated problems and plans for addressing them; and information on how project outcomes will advance or impact current technologies or capabilities.

ii. Budget information categorized by both object class and project.

iii. If applicable, include a certification that no patentable inventions were created during the budget period.

iv. Updates to the Information Protection Plan and Researcher Safety Plan as needed.

If the performance report contains any information that is deemed proprietary, the Recipient will denote the beginning and ending of such information with the following heading: ******PROPRIETARY INFORMATION******

2. Final Performance Report. The Recipient shall submit the Final Performance Report to the DHS Grants Officer no later than 90 days after the expiration of the Project Period (See Section I). The Final Performance Report must include an executive summary and final summary abstracts for each sub-project shall be submitted via the GrantSolutions ***Grant Notes*** feature using the **Grant Note submission guidance** found here: https://www.grantsolutions.gov/support/granteeUsers.html.

Monitoring

DHS, through its 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. During site visits, DHS will review grant recipients' files related to the grant-funded program.

As part of any monitoring and program evaluation activities, grant recipients must permit DHS, upon reasonable notice, to review grant-related records and to interview the organization's staff and clients regarding the program, and to respond in a timely and accurate manner to DHS requests for information relating to their grant program.

Close Out Reporting Requirements.

1. Within 90 days after the end of the period of performance, or after an amendment has been issued to close out a grant, whichever comes first, recipients must submit a final FFR and final progress report detailing all accomplishments and a qualitative summary of the impact of those accomplishments throughout the period of performance. The final report must include: Development of a Reference Architecture for SOAR implementation capabilities across SLTT; Pilot(s) metrics report; SOAR requirements definition; Data model and data format for orchestration and automation services and SOAR implementation risk profile reports.

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 *the Grants and Financial Assistance Division* a close-out notice will be completed to close out the grant. The notice will indicate the period of performance as closed, list any remaining funds that will be deobligated, and address the requirement of maintaining the grant records for three years from the date of the final FFR.

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

G. DHS Awarding Agency Contact Information

Contact and Resource Information
The **Grants Officer** is the DHS official that has the full authority to negotiate, administer and execute all terms and conditions of this Award in concurrence with the Program Officer.

Stephanie Dawkins
Office of Procurement Operations (MGMT OPO)
Grants and Financial Assistance Division
Phone: (202) 447-0495
Email: stephanie.dawkins@hq.dhs.gov

The **Program Officer** is the DHS staff member responsible for monitoring the completion of work and technical performance of the projects or activities described in the Program Narrative Statement.

Shawn Pindell
Cybersecurity and Infrastructure Security Agency
Phone: (703) 705-6243
Email: shawn.pindell@hq.dhs.gov

H. Additional Information

Extensions

Extensions to this program are allowed. Applicants may request a no-cost extension in order 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.

Disclosure: Risk Assessment Evaluation

DHS staff will evaluate the risks to the program posed by each applicant, including conducting due diligence to ensure an applicant's ability to manage federal funds. This evaluation is in addition to the evaluation of the applicant's eligibility and the quality of its application on the basis of the Selection Criteria, and results from this evaluation may assist funding decisions. If an award is made, DHS may apply special conditions that correspond to the degree of risk of the award.

In evaluating risks, DHS may consider the following:

- Financial stability;
- Quality of management systems and ability to meet the management standards prescribed in applicable OMB Guidance;
- Applicant's record in managing previous DHS awards, cooperative agreements, or procurement awards, including:
    1. Timeliness of compliance with applicable reporting requirements
    2. Accuracy of data reported
    3. Conformance to the terms and conditions of previous federal awards
    4. If applicable, the extent to which any previously awarded amounts will be expended prior to future awards
    5. Information available through OMB-designated repositories of government-wide eligibility qualification or financial integrity information, such as: Federal Awardee Performance and Integrity Information System (FAPIIS), Duns and SAM
    6. Reports and findings from single audits performed under Subpart F – Audit Requirements, 2 C.F.R. Part 200 and findings and reports of any other available audits
    7. Applicant organization's annual report
    8. Publicly available information, including information from the applicant organization's website
    9. Applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on award recipients.

In addition, organizations who have not received prior DHS Grants and Financial Assistance Division (GFAD) awards may be required to complete a risk assessment questionnaire as part of the pre-award financial and administrative review.

Applicant Disclosure of High Risk Status

Applicants are to disclose if they are currently designated as high risk by a federal awarding agency. This includes, but is not limited to, any status requiring additional oversight by a federal awarding agency due to past programmatic, administrative or financial concerns. If an applicant is designated as high risk by a federal awarding agency, it should provide an explanation with the application package and include the following information:

- The federal awarding agency that assigned the high risk status;
- The federal awarding agency's point of contact for the risk status, including name, phone number and email address;
- Date of the risk status designation;
- Reason(s) for the risk status.

DHS seeks this information to ensure appropriate federal oversight of all grant awards. The disclosure of an organization's risk status does not disqualify it from receiving an award; however additional grant oversight may be required. If necessary, this information will be provided in the award documentation. Failure to disclose high risk status may result in award termination or other remedies.

Other

i. Prior Approval

The Recipient shall not, without the prior written approval of the DHS, request reimbursement, incur costs or obligate funds for any purpose pertaining to the operation of the project, program, or activities prior to the approved Budget Period.

ii. Budget Revisions

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

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

c. 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.

iii. Post-award program income

In the event program income becomes available to the recipient post-award, it is the recipient's responsibility to notify the DHS Grants Officer to explain how that development occurred, as part of their request for guidance and/or approval. The Grants Officer will review approval requests for program income on a case-by-case basis; approval is not automatic. Consistent with the policy and processes outlined in 2 C.F.R. Part 200, pertinent guidance and options, as determined by the type of recipient and circumstances involved, may be approved by the Grant Officer. If approval is granted, an award modification will be issued with an explanatory note in the remarks section of the face page concerning guidance and/or options pertaining to the recipient's approved request. All instances of program income shall be listed in the progress and financial reports.



CISA
CYBER+INFRASTRUCTURE

State, Local, Tribal and Territorial (SLTT)

Indicators of Compromise Automation Pilot

Program Work Details – Appendix A

1 Purpose

The purpose of this financial assistance action is to establish a pilot to establish a State, Local, Tribal and Territorial (SLTT) Grant that will focus on the use of automation to enhance the use of threat Indicators of Compromise (IOC) at the state and local levels. In addition, the pilot will identify key areas for integration and automation at machine speed, potential reduction of manual tasks by humans, and actionable information sharing across enterprises and SLTT. The pilot will also identify orchestration services needed to integrate the activities of sensing, sense-making, decision-making, and acting. The grant recipient may select up to five states and/or localities to participate in the pilot project

1.1 Objectives

- Generation of threat IOCs faster than the legacy process.
- Action upon IOCs within minutes of receipt.
- Reduce time spent on repetitive tasks.
- Provide generation, enrichment and scoring of IOCs.
- Receipt, remediation and response to IOCs.
- Demonstrate the use of Security Orchestration, Automation, and Response (SOAR) operational procedures and capabilities combined with information sharing to make data more actionable and enable consistent execution at and across SLTT levels.
- Development of repeatable processes for orchestration and automation services that bridge existing SLTT policies with SOAR capabilities.

1.2 Assumptions and Constraints

This section defines the broad assumptions and constraints, which the recipient shall consider in developing its technical solution.

- Services shall be consistent with industry best practices and shall conform to Department of Homeland Security (DHS) principles, Technical Reference Models and the Systems Engineering Life Cycle.
- Services shall be compliant with the DHS Enterprise Security directives, Federal Information Security Management/Modernization Act, and other applicable Federal, DHS and DHS security, acquisition, information systems and asset management laws, regulations, rules, and policies.
- Services shall be compliant with DHS Enterprise Security Operations: Governance Model.

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 shall not leave DHS infrastructure and/or facilities, be photocopied, or pen copied verbatim.

All internal Cyber Security Infrastructure Agency (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 shall 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*.

All services provided under this financial assistance award shall be compliant with the most current version of DHS information security policies, as documented in DHS Management Directive MD4300.1, *Information Technology Systems Security*, and in DHS 4300A, *Sensitive Systems Handbook*.

3 Scope of Work

The scope consists of support tasks and duties needed to support the use of automation to enhance and speed the evaluation of threat indicators of compromise at the SLTT government level. The scope of this grant will engage with a select number of states (up to 5) to identify new models, frameworks, strategies, processes and accompanying policies that can be applies by SLTT.

4 Specific Tasks and Deliverables

4.1 Functional Area 1: Program Management

4.1.1 Task 1 – Transition

Within thirty (30) days of award, the Recipient shall provide an orientation to introduce Government personnel, programs, and users to the Recipient leadership and services team, tools, methodologies, business processes, etc.

4.1.2 Task 2 – Task Management and Control

The Recipient shall provide the management and functional support needed to manage all aspects of delivery of services defined in this statement of work (SOW). The Recipient shall identify a Program Officer (PO), who shall provide program management activities including, but not limited to: transition planning, project planning, resource management, quality assurance, risk management, status and problem reporting and administrative support.

Prepare a Program Management Plan

The Recipient shall present a detailed final Program Management Plan (PMP) that outlines how the Cooperative Agreement/Grant will be executed. The PMP shall describe the technical approach, organizational resources, number of personnel, key personnel, milestones, and management controls to be employed to meet the cost obligated, performance and schedule of requirements throughout execution. The PMP will include an outline of deliverables, schedule, and budget. The PMP will be considered an accountable document outlining the work and expectations between the

Government and Recipient regarding the execution of the work listed in the Cooperative Agreement. The PMP shall be provided to the Government Program Officer for approval within fifteen (15 days) of award. Any request for work to be done from the government that the Recipient determines falls outside of this Cooperative Agreement/Grant should be identified and discussed with the Government's Program Officer prior to committing any additional resources.

Prepare a Communications Plan

The Recipient shall be responsible for the delivery of the Communications Plan and make updates as required throughout the contract term to ensure information is current. The Recipient shall propose a draft Communications Plan and present a finalized Communications Plan for stakeholder contact efforts within thirty (30) working days after award.

Prepare a Quality Assurance Plan

The Recipient shall provide a Quality Assurance Plan to the Government Program Officer for approval within fifteen (15) days after the kick-off meeting. The plan shall document the organizational structure, details on each employee's responsibilities, and the qualifications an employee needs to fulfill those responsibilities. The document shall specify practices, quality standards, resources, specifications, sequence of activities that relate to a particular product, service or project established in order to ensure products and procedures meet stakeholder expectations and needs. The Recipient shall periodically update the Quality Assurance Plan as changes in program processes are identified.

Staffing/Resources/Key Personnel

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

The Recipient shall ensure that its staff maintains any required professional certifications, accreditations, and proficiency relative to their areas of expertise. The Recipient shall retain documentation of such records. The Government will not pay expenses incurred by the Recipient or by individual employees to meet professional certifications and accreditations requirement.

All Recipient staff shall be fully proficient in the areas in which they work. All personnel shall routinely:

1. Maintain professional certifications.
2. Keep current with advances in relevant cybersecurity awareness and share this knowledge with other SLTT and Government DHS 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 capabilities will be shared with the Government/DHS Program Officer for review and approval before implementation.
4. Respond promptly, professionally and courteously to Government requests for assistance and advice on in-scope DHS cybersecurity topics.

5. Freely provide knowledge transfer of work products and cybersecurity expertise associated with services.

4.1.2.1 Kick-off Meeting

The Recipient shall hold a technical kickoff meeting within ten (10) business days following award. The Recipient shall present, for review and approval by the Government, the details of the intended transition approach, work plan, and schedule and the plan for staffing to enable full assumption of services by the end of the sixty (60) day transition period. The Recipient shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least five (5) calendar days prior to the meeting), and meeting minutes shall be provided to Government attendees within three (3) business days after the meeting.

4.1.2.2 In-Progress Review (IPR)

The Recipient shall conduct Weekly In-Progress Review Meetings via teleconference with the Government Program Officer to discuss program and project status, performance measures, existing or potential problems, accomplishments, and projected tasks and milestones. In addition, the Recipient shall:

1. Prepare and maintain the Project Plan(s) - For each project, the Recipient shall prepare a Project Plan that generally describes the technical approach, value added, output or deliverables, organizational resources involved, risk management, communication management, scope, budget and schedule with deadlines and milestones.
2. Measure, track and evaluate progress against the project plan.
3. Prepare and maintain a Publication Outlook Report.
4. Maintain Stakeholder Engagement Outlook Report.
5. Provide a summary of trips taken, conferences attended, etc. (attach trip reports for reporting period) - The Recipient shall provide the Government with a Trip Report five (5) days after travel is completed. The Recipient shall identify the travel, to include: the name of the employee, location of travel, duration of trip, Point of Contact at travel location, task that the travel supports, benefit to the Government, accomplishments/lessons learned, and itemized listing of expenses, both planned and actual.

4.1.2.3 Program Management Review (PMR)

The Recipient shall conduct monthly strategic review meetings via teleconference with the Government Program Officer and DHS Leadership team to monitor progress of the program and its technology implementation from a strategic level and make sure that objectives are on track. Monthly 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 shall:

1. Work with the PO to institute a process of collecting and reviewing information to help make long-range strategic decisions on a monthly basis.
2. Recipient will define its program and technology strategy, or direction of initiatives.
3. Recipient executive leadership shall present a review of the strategy map/plan, offering perspectives on the program and initiatives it must prioritize.

4. Recipient shall ensure that upgrades, improvements and program services move towards an agreed-upon end.
5. Monthly 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.

4.1.2.4 Reporting

The Recipient shall provide a monthly status report on the full range of services required under this agreement to the PO using MS Office Suite applications, by the tenth (10^{th}) of each month via electronic mail to the PO and submission via the GrantSolutions Grant Note feature using the **Grant Note submission guidance** found here: https://www.grantsolutions.gov/support/granteeUsers.html. In addition to progress reporting, the Recipient shall inform the designated Government PO of any issues, problems and recommendations for the overall efficient accomplishment of goals. Recommendations for actions that need to be taken by DHS staff, shall be clearly defined and communicated to the responsible DHS party, and have identified dates for completion.

For special projects, the Recipient shall provide monthly project status reports focused on the successful accomplishment of major milestones/deliverables within the planned project schedule and costs. Project reporting shall also address any issues, problems, risks or concerns that could negatively impact the project.

The Recipient shall provide status reports including self-evaluations and management briefings to document support services activities, summarize accomplishments, present analyses of major challenges and offer innovative solutions to improve weaknesses based on established performance measures. The status of all deliverables shall be monitored and presentations shall describe achievements, service levels and results in meeting objectives.

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

1. Activities during reporting period, by task (Include: On-going activities, new activities, completed activities), *progress* to date on all activities). Start each section with a brief description of the task.
2. Schedule (Shows major tasks, milestones, and deliverables, planned and actual start and completion dates for each).
3. Monthly Performance measures and metrics.
4. Problems and corrective actions taken. Also include stakeholder requirements, issues or concerns and proposed resolutions to address them.
5. Financial Status Report (to include: funding burn rates (Monthly) - Budget, Forecast, Estimate At Completion (EAC), Budget vs EAC variance).
6. Earned Value Management (EVM) statistics.
7. Comparison data / cost sharing between states and the Federal Government
8. Personnel gains, losses and status (security clearance, etc.).
9. Issues or key risks, including constraints (e.g., cost, schedule, etc.,) and assumptions, and planned responses for each.
10. Challenges and Government actions required.

4.1.2.5 Meetings

The Recipient shall support recurring status meetings, reviews, and conferences by preparing and delivering meeting agendas, meeting minutes, presentation materials, and an action item list for each meeting, review and/or conference. The Recipient shall notify the Government of its readiness prior to the start of any meeting, review, and/or conference.

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

a. The Recipient shall propose a date/purpose for a meeting, review and/or conference for the Program Officer's approval.
b. For all presentations, the Government reserves the right to revise the agenda and/or presentation materials. The Recipient shall provide appropriate personnel available to respond to Government questions. The Recipient shall prepare and deliver a summary of open, pending, and closed action items and presentation materials two (2) days prior to the start of each scheduled conference, meeting, and/or review.
c. The Recipient shall record and submit minutes. The Recipient shall track action items. Each assigned action item shall have a due date and responsible Government or Recipient person(s) assigned, who shall 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 shall be developed for closure.

4.1.3 Program Management Deliverables

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

Deliverable	Due Date	Type
Program Management Plan	Draft: Fifteen (15) business days after award Final: Fifteen (15) business Days after receipt of Government comments Update: Semi-annually	Formal
Communications Plan	Draft: Thirty (30) business Days after Award Final: Fifteen (15) business Days after Government comments	Formal
Quality Assurance Plan	Draft: At Task Order Kickoff Meeting Final: Fifteen (15) business Days after Government Comments	Formal
Risk Management Plan	Draft: At Kickoff Meeting Final: (Fifteen) 15 business Days after Government Comments	Formal
Monthly Status Report	Initial: On the 10th of each Month, or on the first business day following the 10th if the 10th falls on a non-business day), commencing sixty (60) calendar days after TO Award	Formal
Meeting Agenda, Minutes, Action Items	Agenda: Five (5) business days prior to meeting Minutes and Action Items: Three (3) business days after meetings	Formal
Transition Lessons Learned	Draft: Fifteen (15) Business Days after the completion of transition Final: Thirty (30) Business Days after the completion of the transition	Formal