PIID: 70RSAT22D00000001- 70RCSJ24FR0000043

FEDERALLY FUNDED RESEARCH AND DEVELOPMENT (FFRDC) TECHNICAL EXECUTION PLAN (TEP)

U.S. Department of Homeland Security

Title: Climate Change: E.O. 14008 Response

Component/Office: Cybersecurity and Infrastructure Security Agency (CISA)
Directorate/Division: National Risk Management Center (NRMC)
Homeland Security Systems Operational Analysis Center (HSOAC)

Version: 1.1

Date: January 3. 2024

1. Challenge

The President's Executive Order on Tackling the Climate Crisis at Home and Abroad ("the Executive Order") issued on January 27, 2021 directs the Secretary of Homeland Security to "consider the implications of climate change to National Critical Functions."[1] The National Critical Functions (NCFs) represent "the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Climate change creates both risks and opportunities associated with ensuring the security and resilience of service provisioning across critical infrastructure systems as evaluated through the lens of the NCFs. Understanding of these risks from climate change will necessarily improve as new information and science emerges, and the risk assessments and mitigation strategies will necessarily need to evolve to reflect this new information as it becomes available.

2. Outcome(s)

In responding to the Executive Order, CISA seeks to understand how the effects of climate change will affect United States security and economic prosperity through impacts on the National Critical Functions of critical infrastructure in the United States. With this information, CISA can work with critical infrastructure owners and operators to identify investment

---

[1] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/27/executive-order-on-tackling-the-climate-crisis-at-home-and-abroad/*

opportunities and strategies to mitigate these risks and increase resilience of critical infrastructure in the United States.

3. Background

CISA's mission is to lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. CISA includes the CISA Mission Enabling Offices and four Divisions: the Cybersecurity Division (CSD), the Emergency Communications Division (ECD), the Infrastructure Security Division (ISD), the Stakeholder Engagement Division (SED), as well as, the National Risk Management Center (NRMC), which are headquartered with the National Capital Region (NCR).

Sec.103 (e) of Executive Order 14008 states that:

> *(e) The Secretary of Homeland Security shall consider the implications of climate change in the Arctic, along our Nation's borders, and to National Critical Functions, including any relevant information from the Climate Risk Analysis described in subsection (c) of this section, in developing relevant strategy, planning, and programming documents and processes. Starting in January 2022, the Secretary of Homeland Security shall provide an annual update, through the National Security Council, on the progress made in incorporating the homeland security implications of climate change into these documents and processes.*

The Secretary has delegated the responsibility for performing the annual assessment of the NCFs to CISA. The Homeland Security Operations and Analysis Center (HSOAC) has assisted the NRMC in the development of an analytic framework, analysis of risk to NCFs, and the preparation of the 2022, 2023, and 2024 drafts of the report as required by the Executive Order. The response included an analysis of how flooding, extreme tides and sea-level rise, tropical cyclones and hurricanes, severe storm systems, extreme cold, extreme heat, wildfire, and drought are expected to impact the NCFs in the years 2050, and 2100 under the following two scenario conditions:

- High Emissions scenario: This scenario reflects the projected global mean temperature change by 2100 in the event of a sudden significant increase in future global emissions and/or a higher climate sensitivity that results in higher magnitudes of climate change per unit of emissions. This is equivalent to global warming of approximately 5 C (9 F) by the end of the century.
- Current Policies scenario: This scenario reflects the projected global mean temperature change by 2100 given current global emissions levels and national commitments to emissions reductions. This is equivalent to global warming of approximately 3 C (5.4 F) by the end of the century.

HSOAC also provided information on climate risk mitigation strategies and developed public outreach materials communicating the results in a digestible format.

Should there be any revisions to the NCF decompositions since the 2024 analysis, CISA will provide HSOAC with the updated NCF decompositions. In addition, new information and science is regularly emerging in the form of new studies on the effects of climate change, new analysis of NCFs by CISA, and results from analysis supporting annual responses to the Executive Order. It is imperative that each annual response and the methods used in the analysis supporting it be improved to reflect the emerging science and knowledge from these sources. These efforts must be consistent with and complementary to a) other initiatives defined by the President's Executive Order on climate change; b) infrastructure proposals included in the administration's American Jobs Plan, federal responsibilities under the U.S. Global Change Act of 1990; and c) other critical infrastructure and climate change efforts of the U.S. Government.

In completing this task, HSOAC will serve as a trusted partner for DHS delivering independent analysis to support the task objectives by leveraging its institutional capabilities as an FFRDC to maintain staff with knowledge and expertise of these topics of interests to DHS and maintain institutional knowledge of the approaches DHS has developed and used to respond to the Executive Order.

4. Task Objective(s)

To support CISA in meeting the challenging and achieving the outcomes for this Task, HSOAC will:

- Support CISA with analysis to develop annual responses to E.O. 14008 response that incorporate new scientific knowledge and data with each iteration of the response including updates and refinements to the risk assessment methodology, updates CISA makes to NCF decompositions, and new information about risk from climate change to all 55 National Critical Functions.
- Provide an updated assessment of cascading impacts, dependencies, and interdependencies that climate-change induced disruptions or failures of the NCFs may have on the execution of other NCFs.
- Conduct regional-level climate risk analysis for high priority regions selected in coordination with NRMC and develop communications materials for those regions.
- Provide additional analytic support to NRMC to address emerging issues and provide additional or more in-depth analysis and other materials related to climate change-related risks to NCFs and potential mitigation measures identified by HSOAC and CISA through analysis contributing to the E.O. response.

5. Technical Approach / Analytic Methodology

- A draft 2025 updated response to the Executive Order and accompanying report. The report shall summarize the activities and resulting findings from Tasks 1 and Task 2.
- A final 2025 update response that will be generated after NRMC has reviewed and commented on the draft update.
- A draft technical document that describes the methodology and provides more detailed explanations of the risk ratings for all 55 NCFs.
- A final briefing summarizing the findings of the final EO response and accompanying report.

5.3 TASK THREE: Prioritize regional-level analysis of climate change-related risks

HSOAC shall prioritize CISA's ten regions to assist CISA in selecting which regions to select for regional-level analysis of climate change-related risks to the NCFs for the 2026 annual response. This analysis will determine the prioritization order for conducting region-specific assessments of climate change's impacts to the NCFs. The highest priority region shall be identified in coordination with NRMC and shall be based on factors including but not limited to: expected underlying risk based on exposure to climate drivers and other available evidence, availability of regional-level climate change data and other information, and whether the region has not already participated in a Regional Resiliency Assessment Program (RRAP) or similar effort.

5.4 TASK FOUR: Begin research and development of rough draft of CISA response to E.O. 14008 for year 2026.

HSOAC shall conduct initial research needed for the development of the CISA response to E.O. 14008 for year 2026. HSOAC shall conduct a review of the methodology and data sources employed for the 2025 E.O response and any feedback received on the 2025 EO response. HSOAC shall prepare a brief memorandum to NRMC identifying lessons learned as a result of the 2025 effort, methodological changes to be implemented, and new data sources including realized risk to the NCFs as a result of climate change. HSOAC shall prepare an initial rough draft of the 2026 E.O response which draws on these methodological and source improvements.

This task will generate the following deliverables:

- A draft 2026 response to the Executive Order that incorporates lessons learned from the 2025 effort, new data sources, and updates to HSOAC's methodological approach.

5.5 TASK FIVE: Develop outreach materials

HSOAC shall develop outreach materials for the two regions selected for the 2025 EO 14008 response. These outreach materials shall consist of:

- A summary of findings included within the 2025 EO 14008 response for each region,

should the region confirm a desire for such product. If the requirement is validated by the region, these materials will be designed for regional staff to share key findings for stakeholders within each region.

- Other outreach materials related to mitigation/outreach as resources allow.

5.6 TASK SIX: Develop the 2026 CISA response to E.O. 14008, conduct regional-level risk analysis on up to two (2) priority CISA regions, and develop progressive mitigation materials [OPTIONAL TASK].

HSOAC shall leverage the refined and improved methodology and draft 2026 EO response to E.O 14008 and an accompanying technical report. HSOAC shall incorporate new information, including updated climate science research, real world manifestation of risk from climate change to the NCFs, changes to the NCFs resulting from technological, social, and other developments, and newly available information from NRMC including development of the NCFs, decomposition, the Risk Architecture, and changes to federal government programs and priorities. HSOAC shall

- Finalize the draft Executive Order for the year of 2026 developed in Task 5 to ensure its timely submission.
- Provide a technical document that describes the methodology used and provides more detailed explanations of the risk ratings for all 55 NCFs.
- Provide a briefing that summarizes the findings for the 2026 EO response.
- Begin draft response to E.O. Order 14008 for year 2027 to include an in-depth analysis of at least two CISA regions. This effort will include a review of the methodology and data sources employed for the 2024, 2025, and 2026 E.O response and any feedback received on the 2024 and 2025 EO responses. HSOAC shall prepare a brief memorandum to NRMC identifying lessons learned as a result of the 2025 effort, methodological changes to be implemented, and new data sources including realized risk to the NCFs as a result of climate change. HSOAC shall prepare an initial rough draft of the 2027 E.O response which draws on these methodological and source improvements.

HSOAC shall develop risk communications and outreach materials that incorporate and communicate findings from the other efforts in this task. These shall include materials for the region or regions addressed in the regional analyses. To the extent resources allow, HSOAC shall also produce other progressive materials to address gaps identified in the prior year's outreach materials (e.g., NCFs which were not covered in other materials or providing interactive as opposed to static communication tools).

This task will generate the following deliverables:

- A final 2026 update response that will be generated after NRMC has reviewed and

commented on the draft update provided in Task Five.

- A final briefing summarizing the findings of the final EO response and accompanying report.
- A technical document that describes the methodology used and provides more detailed explanations of the risk ratings for all 55 NCFs.
- A draft 2027 response to the Executive Order that incorporates lessons learned from the 2026 effort, new data sources, and updates to HSOAC's methodological approach.
- Regional-level and progressive communication and outreach materials addressing known gaps in existing materials and/or incorporating new analyses.

6. Key Words

Type of Work

Risk assessment; risk analysis; risk mitigation; climate change analysis; analysis of alternatives; scenario analysis; failure analysis; feasibility analysis; material flows analysis; benefit cost analysis; cost-effectiveness analysis

Benefit of Work

Improve understanding of drivers of risk to the National Critical Functions from climate change and how climate change may impact the National Critical Functions; improve the ability to assess risk to the National Critical Functions from climate change; identify which National Critical Functions are most at risk from climate change; identify means and opportunities to mitigate risk to the National Critical Functions; generate risk analysis products and tools for critical infrastructure managers

Subject of Interest

National Critical Functions; critical infrastructure; climate change; risk assessment; risk mitigation; risk management; national security impact; national economic impact

7. Focus Area and Mission Alignment

Table 1 below aligns the percent of the total projected staff years of technical effort (STE) allocations to the IDIQ focus areas and DHS Quadrennial Homeland Security Review (QHSR) missions.

FFRDC proposed total STE: Base 1.83; Option 1.92

DHS Management Directive 143-04, "Establishing or Contracting with FFRDCs and National Laboratories" defines a STE as 1,810 hours of paid effort for technical services.

Table 1: Focus Areas to the QHSR Mission Areas Relationship Matrix

At the intersection of the appropriate Focus Area row and QHSR Mission column, enter a percentage of the total STE. **HSOAC Focus Areas**	Mission 1: Counter Terrorism and Prevent Threats	Mission 2: Secure and Manage Our Borders	Mission 3: Administer the Nation's Immigration System	Mission 4: Secure Cyberspace and Critical Infrastructure	Mission 5: Build a Resilient Nation and Respond to Incidents	Mission 6: Combat Crimes of Exploitation and Protect Victims
1: Acquisition Studies	0%	0%	0%	0%	0%	0%
2: Preparedness, Response, and Recovery	0%	0%	0%	0%	0%	0%
3: Innovation and Technology Acceleration	0%	0%	0%	0%	0%	0%
4: Homeland Security Threat and Opportunity Studies	0%	0%	0%	0%	100%	0%
5: Personnel Policy and Management Studies	0%	0%	0%	0%	0%	0%
6: Operational Studies	0%	0%	0%	0%	0%	0%
7: Organizational Studies	0%	0%	0%	0%	0%	0%
8: Regulatory, Doctrine, and Policy Studies	0%	0%	0%	0%	0%	0%
9: Research and Development Studies	0%	0%	0%	0%	0%	0%

8. Deliverables and Schedule

The FFRDC shall provide the following deliverables (predicated in calendar days) according to Table 2 below, and the most current Project Management Plan (PMP), as approved by the Project Manager and DHS Contracting Officer or COR.

<<Please include anything that the FFRDCs plan to deliver as part of this task.>>

Table 2: Deliverables

Scope Ref.	Deliverable Name	Delivery Date
5.0.1	Task Order Project Kickoff Briefing/ Post Award Conference	15 days after fitness clearance
5.0.2	Project Management Plan (PMP) (Draft)	30 days after fitness clearance
5.0.3	Project Management Plan (PMP) (Final)	45 days after fitness clearance
5.1	Methodological Approach Briefing	30 days after fitness clearance
5.2.1	Draft Update for 2025 EO Response & updates as needed	11/01/2024, if timely fitness clearance
5.2.2	Final 2025 EO Response Detailing Analysis of Impact of Climate Change on 55 NCFs Using Current Decompositions	12/02/2024, if timely fitness clearance
5.2.3	Draft Technical Report Documenting the Risk Assessment	12/15/2024, if timely fitness clearance
5.2.4	Briefing on Findings Related to 2025 EO Response	1/30/2025, if timely fitness clearance
5.5	Outreach Materials for Regions	By 30 days prior to Base expiration, if timely fitness clearance
5.6	[Option] Final Updated 2026 EO Response	December 2025, if timely fitness clearance
	[Option] Final Briefing on Findings Related to 2026 EO Response	January 2025, if timely fitness clearance
	[Option Updated technical report documenting the risk assessment of Impact of climate change on 55 NCFs	January 2025, if timely fitness clearance
	[Option] Draft of 2027 E.O. response	Within 360 days of award of Option 1, if timely fitness clearance
	[Option] Regional-level and progressive communication and outreach materials	Within 360 days of award of Option 1, if timely fitness clearance
All	Final Task Completion Memo – Final documentation of deliverables and summary of work performed since final report delivered.	End of the period of performance

The FFRDC shall provide all deliverables under this task order directly to the S&T FFRDC PMO

[redacted] the Task Order PM, TPOC, and Task Order COR. An unclassified abstract, 100 to 200 words in length, and at least five keywords, or a completed Standard Form 298, "Report Documentation Page," shall accompany each deliverable as indicated in Table 2. deliverable. Note that the Report Documentation Page will identify the approved release distribution level (e.g., distribution is unlimited; distribution authorized to US Government agencies only; etc.).

The FFRDC shall deliver a monthly status report by the 15th for HSOAC of the following month containing metrics pertaining to financial, schedule, technical progress, deliverable status, and risk information related to the task. The FFRDC task lead and the task order COR as needed will discuss relevant issues in evaluating the task priorities for the next period; and update the program plan as necessary.

9. Travel

Travel may be necessary to meet and coordinate interagency exchanges of information and to collect data for this task. The FFRDC shall provide trip reports, if requested, to the task order COR for all non-local travel within 30 days of completion of travel.

- Total Number of Trips (All Travelers): 0
- Total Number of Travel Days (All Travelers): 0

The task order COR must approve all foreign travel. Foreign travel must be approved at least 30 days (for unclassified visits) or 45 days (for classified visits) in advance of the planned travel event.

Travel, including local non-commuting travel, shall be reimbursed in accordance with the Federal Travel Regulation. Daily commuting costs shall not be reimbursed. Long-distance travel not specified in this Task Order must be pre-approved by the Task Order CO or COR.

10. Period of Performance

The period of performance is the following:

Base Period: 8 months from Task Order execution.

Option Year One: 12 months from Option Exercise.

The total task order period of performance is for 20 months.

Note: The HSOAC IDIQ contract limits task order end dates to 3/23/2028. Also, options and addons cannot be executed on the current IDIQ contract on pre-existing task orders after the IDIQ ordering end date, 3/23/2027.

11. Security Requirements

This Task Order will require access to the following information:

☒ 1. Unclassified, no markings
☒ 2. Sensitive but Unclassified (SBU), For Official Use Only (FOUO)

11.1 The Contractor shall safeguard SBU, FOUO information in accordance with DHS Management Directive 11042.1 and in compliance with all applicable terms and conditions of the contract, including HSAR Class Deviation 15-01 Safeguarding of Sensitive Information. The parties acknowledge that in order to align with current DHS acquisition policy the July 2023 HSAR Class Deviation 15-01, Revision 1 Safeguarding of Controlled Unclassified Information (CUI) clauses are expected to be incorporated via modification to this task order. The parties further acknowledge that any CUI handled, stored or in any way used in the performance of this task order prior to such modification will be safeguarded in the manner applicable to SBU and FOUO information.

11.2 Security requirement # 5 (PCII) – The FFRDC shall comply with all requirements of the Protected Critical Infrastructure Information (PCII) Program set out in the PCII Act, in the implementing regulations published in the Interim Rule, and in the PCII Procedures Manual as they may be amended from time to time, and shall safeguard PCII in accordance with the procedures contained therein.

11.3 Security requirement # 5 (PCII) – The FFRDC shall ensure that each of its employees, consultants, and subcontractors who work on the PCII Program have executed non-disclosure agreements (NDAs) in a form prescribed by the PCII Program Manager. The FFRDC shall ensure that each of its employees, consultants and subcontractors has executed a NDA and agrees that none of its employees, consultants or sub-contractors shall be given access to PCII without having previously executed a NDA.

11.4 Security requirement # 2 (SBU, FOUO) – The FFRDC shall adhere to all applicable government laws, regulations, orders, guides, and directives pertaining to classified, Sensitive But Unclassified (SBU), FOUO, or personally identifiable information. The contractor shall safeguard SBU, FOUO information specifically in accordance with DHS Management Directive 11042.1 and in compliance with HSAR Class Deviation 15-01 Safeguarding of Sensitive Information.

11.5 The contractor shall use Science & Technology or another DHS Components' accredited General Support System (GSS) to accomplish this work, when applicable, until such time as HSSEDI or HSOAC Accredited Enclave solution becomes available. If classified work is required under this Task Order, the Task Order COR shall provide specific guidance to the FFRDC as to which work will be conducted in a classified manner and at which classification level. If such DHS-guidance conflicts with other applicable guidelines (e.g., DOE, DOD, etc.), the FFRDC shall adhere to the more stringent guidelines as determined by the Task Order COR and DHS FFRDC PMO. The FFRDC shall also adhere to other

b. Unclassified work will be performed at the following locations:

Unclassified Work Locations

[redacted]	[redacted]

13. Other Contract Details

In accordance with the language in the FFRDC contract, the following sections are repeated here for awareness and should not be changed. If they are changed, the language in the IDIQ takes precedence.

13.1 FFRDC Personnel

Personnel provided by the FFRDC will have the skills and technical background necessary to successfully complete the tasks described in this plan. The FFRDC shall implement and manage the technical approach, organizational resources, management, and quality controls to be employed to meet the cost, performance and schedule requirements throughout task order execution.

13.2 Food and Drink

The FFRDC shall not charge any expense for food, snacks, or drink as part of holding task-related meetings, conferences, or gatherings; however, this prohibition does not prevent the contractor from charging meals and incidental expenses as part of authorized travel expenses.

13.3 Meetings and Workshops

All necessary conference approvals should take place prior to the FFRDC's attendance at any conference in support of the sponsoring component. The component user should follow the conference approval process per the guidance set-forth under DHS Financial Management Policy Manual (FMPM Section 7.10) and any component-specific policies and procedures and provide a copy of approval(s) to the FFRDC.

The FFRDC may interview and conduct workshops of recognized subject-matter experts,

including non-federal experts, to gather the experts' individual knowledge and experience regarding the current state of the art of the technical issues relating to this task, and to foster the building of a long-term collaboration between the individual subject matter experts and the FFRDC on the issues relating to the experts' areas of expertise. The workshops or other interaction with non-Federal experts will be for the purpose of collecting the views of the individual experts, not to result in a consensus of those experts. The FFRDC shall produce an objective assessment on the technical merits of the data and/or experts' views espoused in these meetings; and include an evaluation of the strengths and weaknesses of the various discussion points provided by individuals.

The FFRDC may organize meetings/workshops related to the task with federal officials on behalf of the user; however, federal government personnel will approve the agenda and will chair any federal intra-agency/inter-agency meetings. The FFRDC shall produce an objective assessment on the technical merits of individual and any consensus findings and recommendations discussed in these meetings; and include an evaluation of their strengths and weaknesses of the various discussion points.

13.4 Inherently Governmental Functions

As defined under FAR subpart 7.503 (d) and additionally as described in the Office of Federal Procurement Policy (OFPP) Letter 11- 0 I, Performance of Inherently Governmental and Critical Functions (76 Fed Reg 56227), the FFRDC may perform certain closely associated with inherently Governmental functions. However, in accordance with Federal Acquisition Regulation (FAR) 7.503(c)(20) and Homeland Security Acquisition Manual 3037.103(e), the FFRDC shall not draft Congressional testimony, responses to Congressional correspondence, or agency responses to audit reports from the Inspector General, the Government Accountability Office, or other Federal audit entity. Furthermore, in accordance with FAR 7.503(c)(12)(ii), FFRDC employees, subcontractors, and/or consultants will not be voting members on any DHS source selections. When applicable, FAR clause 52.203-16, "Preventing Personal Conflicts of Interest," as included in the IDIQ contract, will apply to this Task Order.

13.5 Out of Scope Work

The following types of work are out of scope for the FFRDC to perform. More specific types of work that are out of scope are found in the relevant IDIQ contract:

- Performance of any services and functions as defined under FAR Subpart 7.5 - "Inherently Governmental Functions," specifically subparts 7.503 (a), (b) and (c).
- Performance of any Systems Engineering and Technical Assistance (SETA) type work, particularly where such work is directly for staff augmentation and of a general support nature where the specific type and quantity of deliverables are undefined.

- Preparation of any Independent Government Cost Estimates (IGCEs).
- Participation in any Source Selection Evaluation or any other membership body where voting and/or ranking of proposals will lead to a subsequent monetary or contract award. The FFRDC may provide independent technical evaluation of proposals in support to a Source Selection Evaluation body but may not provide any ranking, voting or other assigned ordering or selection criteria other than commenting on the technical merit of a particular proposal or proposal section(s). Use of the FFRDC in evaluating an offeror's proposal MUST BE DISCLOSED IN THE SOLICITATION OF PROPOSALS and the offeror(s) given the opportunity to affect non-disclosure agreements and/or withdraw their offer(s), otherwise the FFRDC may not participate.
- Delivering recurring compliance training to DHS employees, particularly that which could reasonably be considered staff augmentation services, is not allowed. Training associated with the transfer of skills from the FFRDC to DHS is acceptable, as long as such training is non-recurring (i.e. train the trainer) and is not intended to be part of a formal established training program. Waivers to this may be requested from the FFRDC COR. Seminars, workshops, and short-courses intended to extend the access and awareness of FFRDC research, research methods, and data sets to practitioners across the Homeland Security Enterprise to assist them in improving mission effectiveness and efficiency is permissible.
- Software and/or hardware development or other manufacturing unless such development is associated with a prototype demonstration or other proof of concept system and not intended to be a permanent solution or in response to formal requirements.

14. Publications and Communications Concerning Work Performed

In accordance with the language in the FFRDC contract, the following statement is repeated here for awareness and should not be changed. If it is changed, the language in the IDIQ takes precedence.

The FFRDC shall mark all technical data or computer software pursuant to the terms of the IDIQ Contract. This will include, for copyrighted works, an appropriate notice acknowledging DHS's sponsorship of the work, license rights, and the appropriate copyright notice as detailed in the IDIQ Contract.

The DHS desires widespread dissemination of the results of funded non-sensitive research and does not seek to undermine the independence or objectivity of the FFRDC or FFRDC operator in anyway. The FFRDC therefore will generally seek public release approval for the results of non-sensitive research. Thirty (30) days prior to release, the FFRDC will first ask for the task order COR's and CO's agreement that the research product is suitable for release. The FFRDC contract governs the scope of the review. Specifically, this review is strictly a mechanism by which the

If work at *CISA HQ* is necessary for the services being performed under this Task Order, such facilities will be provided at offices at the appropriate location Parking facilities are not provided. Basic facilities such as work space and associated operating requirements (e.g., phones, desks, utilities, desktop computers, and consumable and general purpose office supplies) will be provided to FFRDC personnel.

CISA will provide the following property to the Contractor for work required under this contract:

- Laptops

The Contractor shall use CISA furnished facilities, property, equipment and supplies only for the performance of work under this contract and shall be responsible for returning all CISA furnished facilities, property, and equipment in good working condition, subject to normal wear and tear.

DHS Furnished Property – a quarterly report of all S&T property should be submitted to the COR |FFRDC of all of the equipment purchased on behalf of the Government, and Government Furnished equipment being utilized by either FFRDC.

Subsequently a yearly report of all Government Furnished Equipment shall be provided to the COR | FFRDC. The COR | FFRDC will need a property form filled out for all S&T Contractor Acquired Equipment /Property or purchases on behalf of the Government for insertion into the S&T property management system (SAMS). This insertion will need to include the property form filled out in its entirety, paid invoice(s) showing the property purchase and a picture of the current state of that property.

a) Additional DHS property will not be provided to the FFRDC unless otherwise agreed. If DHS property is provided to the FFRDC for task performance, the FFRDC shall maintain property records, sending a yearly report of all items currently attached to the task order to the COR|FFRDC and the Program Manager and a disposition of the property must be completed at the end of the period of performance.
b) Before purchasing any individual item equal to or exceeding $5,000 that is required to support technical tasks performed pursuant to this Task Order, that has not already been accepted by the Government with the issuance of the Task Order, the FFRDC shall obtain prior written consent from the Program Manager, DHS IDIQ Contracting Officer, and DHS IDIQ COR. The FFRDC shall maintain any such items according to the IDIQ Contract's property accountability procedures, and FAR Part 45.
c) All DHS/GFP/GFE (IT equipment, building passes etc.) must be returned at the conclusion of the task order in accordance with component's procedures.
d) If any GFP/GFE is not returned, a report of survey must be submitted to the COR and Project Manager, referencing the DHS equipment number, pass or card number, name of individual to whom equipment was issued, and the last known location of property.

Contractors who lose a badge will be required to fill out an additional lost badge form.

16. Invoices

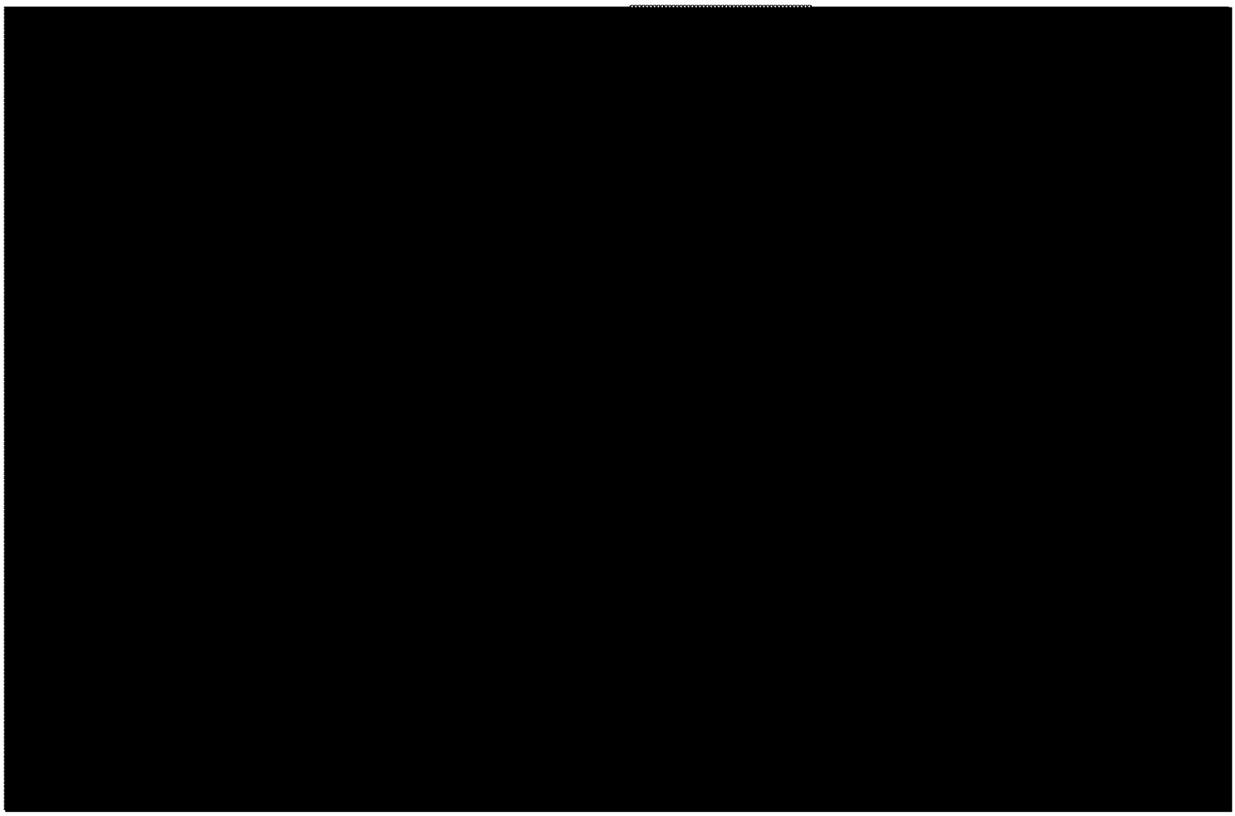
[redacted]

[redacted]

HSOAC invoices will generally be sent on or soon after the 20th of each month.

17. Points of Contact

Government POCs	Corresponding FFRDC POCs
[redacted]	



REFERENCES:

DHS Management Directive 140-01, "*Information Technology System Security Program, Sensitive Systems*"

- DHS 4300A Policy Directive (Version 13.3, February 13, 2023).
- DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018 for NSS Collateral (Unclass, Secret or Top Secret Collateral).
- DHS Sensitive Compartmented Information (SCI) Systems 4300C Instruction Manual, Version 2.1, March 24, 2017 for TS SCI/C-LAN.

3. DHS and CISA ENTERPRISE ARCHITECTURE COMPLIANCE

All solutions and services shall meet DHS and CISA Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security Enterprise (HLS) Architecture (EA) requirements:

- All developed solutions and requirements shall be compliant with the HLSEA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the CISA Chief Data Officer for review, approval and insertion into the DHS Data ReferenceModel and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards will complywith the DHS Data Management Policy MD 103-01 and CISA's Enterprise Data Management Program Policy and all data-related artifacts will be developed and validated according to DHS and CISA data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall bein accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

4. DHS GEOSPATIAL INFORMATION SYSTEM TERMS AND CONDITIONS

All implementations including geospatial data, information, and services shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII), including (but not limited to) the following:

of Life (EoL)"). Software updates and patches shall be either: made available to the government for all products procured under this Contract, replaced upon End of Support (EoS) is reached, or formally waived (in writing) by the DHS Contracting Officer.

d. Supply-Chain Transport

vii. Offerors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill Contract obligations with the Government.

viii. All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the Contract, the period of performance, or one calendar year from the date the activity occurred.

ix. This transit process shall minimize the number of times in route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

x. All records pertaining to the transit, storage, and delivery shall be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

xi. The Offeror is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government.

xii. The Offeror shall provide a packing slip which shall accompany each container or package with the information identifying this solicitation number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

xiii. The Offeror shall send a shipping notification to the intended government recipient; with a copy transmitted via email to the Contracting Officer, or designated representative. This shipping notification shall be sent electronically and will state this solicitation number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Notifications

xiv. The Offeror shall notify DHS Contracting Officer, COR and the Office of the Chief Information Officer and the DHS component Chief Information Officer through the Enterprise Security Operations Center (ESOC) directly of any suspected or

potential violations of Section 889 of the National Defense Authorization Act (NDAA) for Information Communications Technology (ICT) at NDAA_Incidents@hq.dhs.gov.

f. Foreign Equities

The Offeror shall immediately notify the DHS Contracting Officer, COR that will report to the Office of the Chief Security Officer (OCSO) or cognizant component personnel security office regarding any changes to corporate foreign ownership, control, or influence.

7. Section 508 Requirements

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

7.1 Section 508 Requirements for Technology Services

1. When developing or modifying ICT, the Contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation shall occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.

2. When modifying, installing, configuring or integrating commercially available or government-owned ICT, the Contractor shall not reduce the original ICT Item's level of Section 508 conformance.

3. When developing or modifying electronic documents and forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable to the applicable Section 508 standards (including WCAG Level A and AA Level 2.0 Success Criteria) by conducting testing using the test methods published under "Accessibility Tests for Documents" at https://www.dhs.gov/compliance-test-processes.

4. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the accessibility requirements in this work statement.

7.2 Section 508 Deliverables

1. **Section 508 Test Plans**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.

2. **Section 508 Test Results**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.

3. **Section 508 Accessibility Conformance Reports**: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

4. **Other Section 508 Documentation:** The following documentation shall be provided upon request for ICT items offered through this contract:

    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation on how to configure and install the ICT Item to support accessibility.
    - Documentation of core functions that cannot be accessed by persons with disabilities.
    - Documentation of remediation plans to address non-conformance to the Section 508 standards.

8. THE HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12)

- The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the Personal Identity Verification (PIV) credentials as the common means of authentication for access to DHS facilities, networks, and information systems. Personal Identity Verification (PIV) credentials shall be used as the primary means of logical authentication for DHS sensitive systems. The Contractor must use his or her federal issued Personal Identity Verification (PIV) credentials to access DHS resources to include IT applications and physical facility.

- The DHS Security Office shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Representative (COR) all DHS issued Personal Identity Verification (PIV) credentials/identification cards and building passes

that have either expired or have been collected from terminated employees. If a PIV credential/identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the PIV credential, pass or card number, name of individual to who it was issued and the last known location and disposition of the PIV credential, pass or card."

The above language in **section 8** must be included to any SOW if any of the following conditions apply.

1. All **service contracts** (requirements with labor)
2. **Requirement** to use **Personal Identity Verification (PIV) credentials** as the primary means of identification and authentication to Federal information systems and federally controlled facilities incorporated in this procurement.
3. Identity **products and services acquired to further HSPD-12 and ICAM** implementations compliant.

SECURITY

Contractor access to unclassified, but Security Sensitive Information may be required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

Requests for Exception to U.S. Citizenship Requirement

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to citizenship requirements are treated differently from security policy waivers. Exceptions to the U.S. citizenship requirement should be requested by completing a Foreign National Visitor Access Request, DHS Form 11052-1, which is available online or through the DHS Office of the Chief Security Officer (OCSO). Components who have access may file their request via the Foreign National Vetting Management System (FNVMS), a part of the DHS OCSO Integrated Security Management System's (ISMS). For further information regarding the citizenship exception process, contact the DHS CISA

This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).

Post-Award Instructions Regarding Security Requirements for Non-Classified Contracts/Orders

The procedures outlined below shall be followed for the DHS Cybersecurity and Infrastructure Security Agency (CISA), Personnel Security Division (PSD) to process background investigations, Entry on Duty

determinations, and fitness determinations, as required, in a timely and efficient manner.

Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is not optional.

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position-sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations

will be processed through the DHS CISA PSD. Prospective contractor employees shall complete and submit a combination of the below forms to the DHS CISA PSD. The Standard Form (SF) 85 must be completed electronically through the Office of Personnel Management's e-QIP SYSTEM. The SF-85 signature pages and other completed forms must be given to the DHS CISA PSD no less than thirty days before the start date of the contract or thirty (30) days prior to the requested entry on duty date, for all contractor employees whether a replacement, addition, subcontractor employee, or vendor. DHS CISA PSD does not process any requests until the contract has been awarded and released from PRISM to FPDS and ERA by extension.

a. Standard Form (SF) 85 Questionnaire for Public Trust Positions
    i. SF-85P Certification
    ii. SF-85P Authorization for Release of Medical Information
b. FD Form 258 Fingerprint Card (2 copies) or Identity Enrollment Services
c. DHS Form 11000-6 Conditional Access to Sensitive but Unclassified Information Non-Disclosure Agreement
d. DHS Form 11000-9 Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act
e. OF-306 Form, Declaration for Federal Employment

Only complete packages will be accepted by the DHS CISA PSD. Specific instructions on submission of packages will be provided upon award of the contract.

The DHS CISA PSD may, as it deems appropriate, authorize, and grant a favorable Entry on Duty (EOD) decision based on preliminary checks. A favorable EOD decision allows a contractor employee to commence work temporarily prior to the completion of the full background investigation. The granting of a favorable EOD decision shall not be considered as assurance that a favorable fitness determination will follow. In addition, a favorable EOD or fitness determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD or fitness determination by the DHS CISA PSD.

Limited access to Government buildings is allowable without an EOD decision if the Contractor is escorted by a Government employee and the purpose of the visit is to attend a limited number (less than 5) of required briefings or nonrecurring meetings in order to facilitate the transition of a contract. The intent of this statement is to allow a minimum amount of meetings/transition attendances to prepare for a new contract.

The DHS CISA PSD shall be notified of all terminations /resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.

When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level. Contractors who fail to comply with Depa1iment security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

- Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.
- Your POC at the Security Office is:

CISA Chief Security Office

CISA Personnel Division,

E-mailbox: [redacted]