DEPARTMENT OF HOMELAND SECURITY (DHS)
STATEMENT OF WORK (SOW)
FOR
Joint Cyber Defense Collaborative (JCDC)
Operational Technology Support
Request for Quotation Number: 70RCSJ24Q00000095

1.0 GENERAL

1.1 BACKGROUND

1.1.1 The Department of Homeland (DHS) Cybersecurity and Infrastructure Security Agency's (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 (MEOs) and six Divisions: the Cybersecurity Division (CSD), the Emergency Communications Division (ECD), the Integrated Operations Division (IOD), Infrastructure Security Division (ISD), the Stakeholder Engagement Division (SED), as well as, the National Risk Management Center (NRMC), which are headquartered within the National Capital Region (NCR).

1.1.2 CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats through effective coordination and collaboration among a broad spectrum of government and private sector organizations. Within CISA, CSD leads the effort to protect the federal ".gov" domain of civilian government networks and collaborates with the private sector ".com" domain to increase the security of critical networks. CSD's mission is to reduce cyber risk by being the Nation's flagship for cyber defense, incident response, and ensuring the resilience of nationally critical functions by delivering capabilities including technology, information, and analytics to support risk reduction. CSD is comprised of five Subdivisions: Threat Hunting, Vulnerability Management, Mission Engineering, Capacity Building, and the Joint Cyber Defense Collaborative (JCDC).

1.1.3 The JCDC subdivision enables and coordinates operational activities across CSD and engages partner organizations in the execution of those activities. The JCDC subdivision is organized into three operational offices: Planning, Partnerships, and Production. This structure allows for close collaboration including planning towards identified operational outcomes, partnering with operational stakeholders to execute, integrating analytical processes across organizations, and producing technical communications to disseminate to partner communities.

1.1.4 The JCDC's Industrial Controls System (ICS) focused mission was established in 2022 with the purpose of collaborating with key Operational Technology (OT) companies who possess knowledge, visibility, and capabilities of ICS infrastructure. The JCDC's ICS mission is composed of ICS/OT software manufacturers, hardware manufacturers, owners and operators, and integrators. The subject matter experts that have partnered with CISA are charged with building plans around the protection and defense of control systems; collaborating on U.S. government guidance on ICS/OT cybersecurity; and contributing to real time operational fusion across private and public partners in the ICS/OT space.

1.2 SCOPE

1.2.1 The CISA JCDC is seeking a transformation and implementation of the Operational Technology (OT) / Industrial Control Systems (ICS) partnership model to elevate the effectiveness of CISA and the nation's ability to prevent and respond to cyber infrastructure incidents. JCDC requires a broad range of program management, subject matter expertise, stakeholder engagement and management, and service innovation and delivery experience to implement change at scale.

The Contractor will support JCDC and relevant stakeholders in three key areas:

- OT/ICS Program Support
  - Program deployment, execution, and evolution
  - OT/ICS cybersecurity subject matter expertise (SME)
  - Governance and reporting
- Stakeholder Engagement
  - Stakeholder Relationship Management (SRM) administration
  - Stakeholder experience design, execution, and evaluation
  - External stakeholder engagement
  - Internal stakeholder engagement
  - Stakeholder engagement assessment
- OT/ICS Delivery Innovation
  - OT/ICS service development and capability delivery

1.3 OBJECTIVE

1.3.1 The objective is to build on the strategic progress made by JCDC and scale a holistic approach, solutions, processes, and shift from providing stakeholders with transactional experience to more of a relational one. This change boosts JCDC's ability to increase proactive and predictive capabilities to relevant stakeholders such as interagency partners, critical infrastructure owners and operators, and receive continual feedback to maximize return on investments.

1.4 APPLICABLE DOCUMENTS

Compliance documents are not required.

1.4.1 Reference Documents

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).

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 Task One: OT/ICS Program Support

2.1.1 Program Deployment, Execution and Evolution

While engaging partners within dynamic technological and threat environments, CISA JCDC and its stakeholders require an informed and flexible approach in developing the OT/ICS program

strategy, management, and execution.

The Contractor shall:

- Support execution of the overall OT/ICS program strategy in collaboration with internal stakeholders to maximize JCDC OT/ICS program adoption and engagements.
- Facilitate workshops and direct stakeholder engagements to assess and develop current and future OT/ICS Program priorities and supporting activities.
- Support Implementing JCDC OT/ICS program roadmap objectives and activities through the development of short-term and long-term milestones aligned to JCDC priorities.
- Provide regular input and recommendations regarding the OT/ICS Program's current operations and engagement activities.
- Conduct qualitative and quantitative market research to support periodic program benchmarking and assessment.
- Support future strategic development efforts and program operation requirements throughout the execution and maturation of the OT/ICS program.
- Conduct regular stakeholder feedback reviews and gap analyses to assess the state of the OT/ICS Program to develop future goals and roadmaps.

2.1.2 OT/ICS Cybersecurity Subject Matter Expertise (SME)

CISA JCDC requires cybersecurity operational program support, particularly in the of OT/ICS cybersecurity sub-field, to support the management of threat intelligence exchange, cyber defense planning and operations, as well as strategic initiative engagement across program stakeholders.

The Contractor shall:

- Provide Subject Matter Expertise (SME) in OT/ICS cybersecurity to CISA CSD, JCDC, and OT/ICS program leadership, as well as stakeholders across a range of engagements and program support taskings.
- Support the development and administration of virtual communications channels to support the exchange of cyber threat information across diverse stakeholders and participants focused on OT/ICS emerging threats and issues.
- Provide subject matter expertise and stakeholder engagement advisory support to inform cyber operational planners and advance the development and execution of cyber defense plans, particularly as they relate to OT/ICS matters.
- Support the identification and inclusion of external stakeholders in priority cross-CSD and JCDC initiatives. These engagements are strategic in nature intended to raise the cybersecurity baseline (i.e., practice and knowledge) of stakeholders and advance their organization's incident response capabilities and practices.
- Assist in the development or maturation of CISA services by providing OT/ICS cybersecurity subject matter knowledge and experience, particularly regarding CISA-developed, open source, or commercial capabilities aimed at securing OT/ICS assets.
- Support technical training and stakeholder discussions, as well as providing ad-hoc subject-matter expertise to CISA stakeholders and JCDC OT/ICS program staff on OT/ICS- related cyber issues.

2.1.3 Governance and Reporting

CISA JCDC requires continuous program governance support and process improvement to support

the execution, monitoring, and reporting of JCDC OT/ICS Program activities. Activities may include creating charters, operating models, and corresponding SOPs or processes.

The Contractor shall:

- Define new or evolving program support roles and responsibilities to ensure effective program operations and individual accountability.
- Support maturation and refinement of internal program operations and administration
- Develop, maintain, and continuously updating trainings, playbooks, and standard operating procedures (SOPs).
- Develop recommendations and implement methodologies to facilitate program data capture, analysis, reporting, and lessons learned.
- Develop a dashboard or other capabilities to promote transparency and awareness on program activities for internal and external purposes.
- Design and develop executive reports to inform CISA and JCDC leadership decision-making, high-level stakeholder engagements and appearances.
- Create standards, processes, and communication templates for engaging internal and external stakeholders on OT/ICS program initiatives.
- Implementing communications approaches and opportunities (i.e., roadshows, conferences, community briefings, etc.) for engaging stakeholders.
- Support charter development and management of internal leadership and external stakeholder governance bodies or mechanisms to aid the maturation and oversight of the OT/ICS program; develop and maintain artifacts needed to implement the direction of governance bodies for resulting program action.

2.2 Task Two: Stakeholder Engagement

2.2.1 Stakeholder Relationship Management (SRM) Administration

The contractor will provide support to advance the OT/ICS Program's stakeholder engagement, to include CISA and subdivision partners, as well as external public and private entities. This includes maintaining stakeholder engagement management capabilities and processes. Activities will include tracking stakeholder engagement actions to support continuous assessment and opportunity identification.

The Contractor shall:

- Maintain a stakeholder tracking dashboard and underlying Stakeholder Relationship Management (SRM) database to profile individual entities and record activities related to engagements.
- Design, plan, and conduct research leveraging applicable open source and commercial research methodologies to support the stakeholder engagement process.
- Develop a methodology for assessing the relevance, capabilities, and projected involvement of external stakeholders in the OT/ICS program.
- Assess and develop robust stakeholder segments or groupings that are aligned with expectations, offerings, and value propositions for stakeholder engagement with the OT/ICS program.
- Synthesize and summarize stakeholder member base and engagements activities, and recommending improvements and solutions to address identified program gaps.

- Provide continuous assessment of the OT/ICS stakeholder ecosystem for scouting and inclusion, as well as alignment with JCDC priorities and CSD strategy, initiatives, and service offerings.

2.2.2 Stakeholder Experience Design, Execution, and Evaluation

The contractor will support the maturation of JCDC OT/ICS program's stakeholder engagements and introduce new approaches and capabilities, placing stakeholder's needs at the forefront. Activities include recommendation of stakeholder engagements solutions, content style and communications guides, and user-centric approaches to evaluate and evolve engagements.

The Contractor shall:

- Establish communications strategies and a continuous plan to promote stakeholder engagement in JCDC OT/ICS efforts and ensure stakeholders clearly understand the vision, value proposition, and intent of program activities and initiatives.
- Use customer experience and design-thinking industry best practices to advance technical exchange and operational collaboration opportunities with stakeholders.
- Provide design expertise and support to implement approved activities and engagements intended to improve services, applications, websites, and other relevant offerings within and across CISA, CSD, and JCDC.

2.2.3 External Stakeholder Engagement

The contractor will collaborate across external public and private stakeholders to support relationship onboarding and development to advance involvement in OT/ICS program initiatives and activities in fulfillment of CISA and JCDC strategic priorities.

The Contractor shall:

- Support the onboarding of stakeholders and foster subsequent relationship management to strengthen engagement and advance OT/ICS program initiatives.
- Plan, facilitate, and support working-level engagements with internal and external stakeholders to develop and execute JCDC OT/ICS initiatives.
- Develop standard operating procedures, templates, and communications channels (e.g., email mailing lists, online chat, or web-based collaboration platforms) to support stakeholder onboarding and engagement across initiatives.
- Develop collaboration approaches and administer communications channels to enable threat intelligence information sharing and fusion, as well as support cyber defense planning and coordination activities across diverse stakeholder sets.

2.2.4 Internal Stakeholder Engagement

The contractor will support the maintenance and growth of JCDC OT/ICS relationships across CISA, CSD subdivisions and stakeholders, conduct stakeholder analysis, and ongoing mapping and awareness of CSD subdivision services to identify and align opportunities, and enable the integration of subdivision stakeholders into JCDC-led or cross-CISA OT/ICS initiatives. In addition, the contractor will work across CSD subdivisions to contribute to the development of future strategies and priorities for the JCDC OT/ICS Program and CISA OT/ICS strategy.

The Contractor shall:

- Build and foster relationships and connections with internal stakeholders to inform the development of strategic plans and initiatives, service development and delivery, and external stakeholder coordination efforts.
- Map internal stakeholder engagements and service offerings to external stakeholder desires, needs, and capabilities to develop mutually beneficial opportunities and initiatives.

2.2.5 Stakeholder Engagement Assessment

The contractor will collect and analyze stakeholder and operational data to measure and assess program performance to identify improvements. Activities include development or stakeholder engagement key performance indicators (KPI), as well as collection and analysis of qualitative evidence documenting the outcome and impact of stakeholder engagements.

The Contractor shall:

- Work with full cross-functional OT/ICS Program team and internal stakeholders to gather, analyze, and provide insights on internal and external stakeholder engagements aligned to Key Performance Indicators (KPIs).
- Conduct online surveys, direct or group interviews on a routine bases to understand stakeholder engagement and gather qualitative feedback on the overall OT/ICS program, as well as specific activities or initiatives.
- Synthesize and analyze stakeholder feedback, conducting root cause analysis to identify gaps, and drivers of dissatisfaction, as well as developing corresponding suggestions to improve program experience and mission success.

2.3 Task 3: OT/ICS Program Innovation

2.3.1 OT/ICS Service and Capability Delivery

CISA JCDC requires development and delivery of OT/ICS capabilities across CSD's sub-divisions to bring innovative offerings to external stakeholders, as well as facilitate engagements for CISA and inter-agency partners with the OT/ICS community.

The Contractor shall:

- Identify and assess CISA OT/ICS use-cases to evolve current cyber defense approaches and deliver innovative solutions.
- Support the design and development of OT/ICS-focused guidance and publications.
- Enhancing CISA's website and alert notification system to efficiently reach specific audiences regarding OT/ICS-related cyber security incidents and vulnerabilities.
- Support the evolution of CISA Threat Hunting activities and initiatives by facilitating connections with external stakeholders in the OT/ICS communities.
- Develop alternative technical solutions or offerings to capture, communicate, prioritize, and remediate vulnerabilities.
- Work with stakeholders to advance Incident Response (IR) processes and evolve technical solutions (e.g., IR "go-bag") scaled to serve owner/operators.
- Facilitate external stakeholder awareness and participation in OT/ICS opportunities and offerings (e.g., simulations, workshops, assessments).

- Develop and deliver service prototypes and capabilities informed by stakeholder feedback and voluntary testing.

3.0 DELIVERABLES / GOVERNMENT ACCEPTANCE PERIOD

3.1 ACCEPTANCE PERIOD

3.1.1 The Contracting Officer Representative (COR) will review deliverables prior to acceptance and provide the Contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

3.1.2 The COR will have the right to reject or require correction of any deficiencies found in the deliverables. In the event of a rejected deliverable, the COR will notify the Contractor in writing of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

3.1.3 The COR will have 5 business days to review deliverables and make comments. The Contractor shall have 5 business days to make corrections and resubmit.

3.1.4 All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

3.2 DELIVERABLES

3.2.1 The Contractor shall submit all deliverables via email (electronic format with read/write capability using applications that are compatible with DHS workstations (Windows 11 and Microsoft Office Applications)), on the appropriate network (depending on classification) to the POC(s) listed in the table below.

3.2.2 The Contractor shall consider items in **BOLD** as having mandatory due dates.

ITEM	SOW Para	DELIVERABLE / EVENT	DUE	DISTRIBUTION
1	2.1 Program Deployment, Execution, and Evolution	Project Kickoff Meeting	**Within 10 business days of award**	COR, JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
2	All	Weekly Status Reports	**Weekly**	COR, JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
ITEM	**SOW Para**	**DELIVERABLE / EVENT**	**DUE**	**DISTRIBUTION**

3	All	Quarterly Program Management Review	**Within 90 days of award and continuous on a quarterly basis throughout period of performance**	COR, JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
4	All	Business Continuity Plan	**Within 30 days of award** and updated annually	COR, JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
5	2.1.1 Program Deployment, Execution, and Evolution	Qualitative and Quantitative Market Research to Support Program Benchmarking and Assessment	Continuous throughout period of performance (as needed basis)	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
6	2.1.1 Program Deployment, Execution, and Evolution	Project Roadmap Development and Ongoing Execution Support	**Within 30 business days of award**	JCDC Partnerships Leadership
7	2.1.1 Program Deployment, Execution, and Evolution	Facilitate Workshops and Stakeholder Engagements	Continuous throughout period of performance (as needed basis)	JCDC OT/ICS Program Staff
8	2.1.1 Program Deployment, Execution, and Evolution	Stakeholder Feedback Reviews and Gap Analyses	Quarterly or bi-annually, at government program lead's discretion	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
9	2.1.2 OT/ICS Cybersecurity Subject Matter Expertise (SME)	Development and Administration of Virtual Communications Channels (OT/ICS Program-wide)	**Within 60 business days of award** and continuous support throughout period of performance	JCDC OT/ICS Program Staff

10	2.1.3 Governance and Reporting	Functional and Technical Program Documents (e.g. trainings, playbooks, standard operating procedures (SOPs))	Continuous following Kickoff phase and roadmap development	JCDC OT/ICS Program Staff
11	2.1.3 Governance and Reporting	Project Management Plan (including roles and responsibilities of their staff)	**Within 15 business days post kickoff**	COR, JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
12	2.1.3 Governance and Reporting	Methodologies and Process for Program Activity Data Capture, Reporting, and Lessons Learned	**Within 60 business days of award (estimated)**	JCDC OT/ICS Program Staff
ITEM	**SOW Para**	**DELIVERABLE / EVENT**	**DUE**	**DISTRIBUTION**
13	2.1.3 Governance and Reporting	Program Activity Dashboard	**Within 90 days of award (estimated)**	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
14	2.1.3 Governance and Reporting	Communications Standards, Processes, and Templates	**Within 30 days of award (estimated)**	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
15	2.1.3 Governance and Reporting	Community Engagements Opportunities	Continuous throughout period of performance (as needed basis)	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
16	2.1.3 Governance and Reporting	Charter Development: Internal Leadership and External Stakeholder Governance Bodies	**Within 180 days post kickoff**	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
17	2.2.1 Stakeholder Relationship Management Administration	Stakeholder Tracking Dashboard and Stakeholder Relationship Management (SRM) database	**Within 90 days post kickoff** and continuous support throughout period of performance	JCDC OT/ICS Program Staff

18	2.2.1 Stakeholder Relationship Management Administration	Stakeholder Research and Assessment	Continuous throughout period of performance (as needed basis)	JCDC OT/ICS Program Staff
19	2.2.1 Stakeholder Relationship Management Administration	Stakeholder Segmentation and Offering Alignment	**Within 180 days post kickoff,** and re- assessed annually	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
20	2.2.1 Stakeholder Relationship Management Administration	Stakeholder Activity and Program Gap Assessment	**Within 360 days post kickoff**	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
21	2.2.2 Stakeholder Experience Design, Execution, and Evaluation	OT/ICS Program Stakeholder Outreach Communication Plan	**Within 30 days post kickoff** and continuous throughout period of performance (as needed basis)	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
ITEM	**SOW Para**	**DELIVERABLE / EVENT**	**DUE**	**DISTRIBUTION**
22	2.2.2 Stakeholder Experience Design, Execution, and Evaluation	Use customer experience and design thinking best practices to support stakeholder collaboration engagements	Continuous throughout period of performance (as needed basis)	JCDC OT/ICS Program Staff
23	2.2.2 Stakeholder Experience Design, Execution, and Evaluation	Design expertise and support to activities and engagements to improve services, applications, websites and other offerings	Continuous throughout period of performance (as needed basis)	JCDC OT/ICS Program Staff
24	2.2.3 External Stakeholder Engagement	SOPs, templates, and communications channels to support stakeholder onboarding and engagement	**Within 30 days of award** (estimated) and continuous throughout period of performance (as needed basis)	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
25	2.2.3 External Stakeholder Engagement	Plan, facilitate, and support working-level engagements with internal and	Continuous throughout period of performance (as needed basis)	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff

		external stakeholders to develop and execute JCDC OT/ICS initiatives		
26	2.2.3 External Stakeholder Engagement	Development and Administration of Virtual Communications Channels (OT/ICS Threat Information Exchange and Cyber Defense Planning)	**Within 60 business days of award (estimated)** and continuous support throughout period of performance	JCDC OT/ICS Program Staff
27	2.2.4 Internal Stakeholder Engagement	Build and foster relationships and connections with internal stakeholders	Continuous throughout period of performance (as needed basis)	JCDC OT/ICS Program Staff
28	2.2.4 Internal Stakeholder Engagement	Internal Stakeholder Mapping and Offerings Alignment Plan	**Within 60 days of award (estimated)**	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
ITEM	**SOW Para**	**DELIVERABLE / EVENT**	**DUE**	**DISTRIBUTION**
29	2.2.5 Stakeholder Engagement Assessment	Key Performance Indicators (KPIs) Development	**Within 180 days of award (estimated)**	JCDC Partnerships Leadership, JCDC OT/ICS Program Staff
30	2.2.5 Stakeholder Engagement Assessment	Online Surveys and Stakeholder Interviews	Continuous throughout period of performance (as needed basis)	JCDC OT/ICS Program Staff
31	2.3.1 OT/ICS Service and Capability Delivery	CISA OT/ICS Use Case Review	**Within 60 days of award**	JCDC OT/ICS Program Staff
32	2.3.1 OT/ICS Service and Capability Delivery	Stakeholder engagement support to OT/ICS-focused CISA guidance and publication	**Within 90 days of award**	JCDC OT/ICS Program Staff

33	2.3.1 OT/ICS Service and Capability Delivery	Support CISA OT/ICS Website and Alerting Enhancements	**Within 90 days of award**	JCDC OT/ICS Program Staff
34	2.3 OT/ICS Service and Capability Delivery	Stakeholder engagement support to CISA OT/ICS Threat Hunting activities	**Within 90 days of award**	JCDC OT/ICS Program Staff
35	2.3 OT/ICS Service and Capability Delivery	Stakeholder engagement support to CISA OT/ICS Vulnerability Management activities	**Within 90 days of award**	JCDC OT/ICS Program Staff
36	2.3 OT/ICS Service and Capability Delivery	Stakeholder engagement support to CISA OT/ICS Incident Response (IR) solutions	**Within 180 days of award**	JCDC OT/ICS Program Staff
ITEM	**SOW Para**	**DELIVERABLE / EVENT**	**DUE**	**DISTRIBUTION**
37	2.3 OT/ICS Service and Capability Delivery	Stakeholder awareness of CISA OT/ICS opportunities and offerings	**Within 90 days of award**	JCDC OT/ICS Program Staff
38	2.3 OT/ICS Service and Capability Delivery	Stakeholder awareness of CISA OT/ICS service voluntary prototype testing and feedback opportunities	**Within 180 days of award**	JCDC OT/ICS Program Staff

4.0 CONTRACTOR PERSONNEL

4.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW.

4.2 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is appropriately maintained.

4.3 Key Personnel

4.3.1 Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall meet the minimum qualifications described below in the table. The Contractor shall not replace *Key* Contractor personnel without approval from the Contracting Officer.

The following positions are designated as Key for this requirement:

Position	Minimum Education/Experience
ALL TASKS: JCDC Partnerships Branch, Industry Section, OT/ICS Program – Program Manager	Minimum of 15 years of experience, of which at least 10 years must be specialized experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.
TASK 1: JCDC Partnerships Branch, Industry Section, OT/ICS Program – Project Manager III	Minimum of 8 years of experience. This position requires Unclassified Sensitive clearance.
TASK 1: JCDC Partnerships Branch, Industry Section, OT/ICS Program – Subject Matter Expert III	Minimum 8 years of experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.
TASK 2: JCDC Partnerships Branch, Industry Section, OT/ICS Program – Subject Manager Expert III	Minimum of 8 years' experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.

Position	Minimum Education/Experience
TASK 3: JCDC Partnerships Branch, Industry Section, OT/ICS Program – Subject Matter Expert III	Minimum 8 years of experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.
TASK 3: JCDC Partnerships Branch, Industry Section, OT/ICS Program – Subject Matter Expert III	Minimum of 8 years' experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.

4.3.2 Additional Personnel

Position	Minimum Education/Experience
TASK 1: JCDC Partnerships Branch, Industry Section, OT/ICS Program – Program Analyst	Minimum of 4 years of experience. This position requires Unclassified Sensitive clearance.
TASK 2: JCDC Partnerships Branch, Industry Section, OT/ICS Program – Program Analyst	Minimum of 4 years of experience. This position requires Unclassified Sensitive clearance.
TASKS 1&2 (Split): JCDC Partnerships Branch, Industry Section, OT/ICS Program – Project Leader	Minimum of 4 years of experience. This position requires Unclassified Sensitive clearance.

Position	Minimum Education/Experience
TASKS 1&2 (Split): JCDC Partnerships Branch, Industry Section, OT/ICS Program – Communications Specialist	Minimum of 4 years of experience. This position requires Unclassified Sensitive clearance.
TASK 1: JCDC Partnerships Branch, Industry Section, OT/ICS Program –Subject Matter Expert II	Minimum 4 years of experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.
TASK 3: JCDC Partnerships Branch, Industry Section, OT/ICS Program – Subject Matter Expert II	Minimum 4 years of experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.
TASK 3: JCDC Partnerships Branch, Industry Section, OT/ICS Program – Subject Matter Expert II	Minimum 4 years of experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.
TASK 2: JCDC Partnerships Branch, Industry Section, OT/ICS Program –Subject Matter Expert II	Minimum of 4 years' experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.

Position	Minimum Education/Experience
TASK 3: JCDC Partnerships Branch, Industry Section, OT/ICS Front Office –Subject Matter Expert II	Minimum of 4 years' experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.
TASK 3: JCDC Partnerships Branch, Industry Section, OT/ICS Program –Subject Matter Expert II	Minimum of 4 years' experience. This position requires Top Security (TS)/SCI (Sensitive Compartmented Information) clearance.

4.3.3 Contractor Key personnel shall not be assigned by the Contractor to more than one key position for this requirement.

4.3.3.1 Program Manager

4.3.1.1 The Contractor shall provide an onsite Program Manager (PM) who shall be responsible for the performance of the work and provide overall direction to Contractor personnel working under this SOW. The PM shall be a single point of contact for the Contracting Officer and the COR. The name of the Program Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the PM, shall be provided to the Government as part of the Contractor's proposal. The PM is further designated as Key by the Government. During any absence of the PM, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. The PM and all designated alternates shall be able to read, write, speak and understand English. Additionally, the Contractor shall not replace the PM without prior approval from the Contracting Officer.

4.3.1.2 The PM or designated alternate shall be available during normal work hours to meet with the JCDC Associate Director, Deputy Associate Director, or designee, in person or as otherwise agreed upon by JCDC to discuss problem areas. After normal duty hours, the PM or alternate shall be available in accordance with JCDC-approved escalation procedures. In the event of disaster recovery or Continuity of Operations (COOP) events, the PM shall be available during normal hours of operation and during periods of no-notice emergencies, including localized acts of nature, accidents, and military or terrorist attacks to plan, direct, and control the overall management and operational functions specified herein.

4.3.1.3 The PM position requires a minimum of 15 years of experience, of which at least ten years must be specialized experience, including project development from inception to deployment, expertise in the management and control of funds and resources using complex reporting mechanisms, and demonstrated capability in managing multitask contracts of the same or similar

magnitude.

4.3.1.4 The PM is also responsible for management and delivery of the quarterly Program Management Review (PMR). The position requires a Bachelor's degree in Computer Science, Information Systems, Information Assurance, Engineering, Business, or other related discipline. Equivalent years of directly related experience may be considered in lieu of educational requirements. The PM must have intimate knowledge of cybersecurity concepts and policy, and US Government interagency roles and responsibilities.

4.4 Employee Identification

4.0.5 Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level, and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

4.0.5 Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

4.5 Employee Conduct

4.0.5 Contractor's employees shall comply with all applicable Government regulations, policies, and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Program Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

4.0.5 Removing Employees for Misconduct or Security Reasons
The Government may, at its sole discretion (via the Contracting Officer), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

5.0 OTHER APPLICABLE CONDITIONS

5.1 SECURITY

5.1.1 Contractor access to CISA Sensitive Information, systems, networks and reoccurring access to CISA facilities is required under this SOW; therefore, contractor employees will require DHS Fitness

Determination to perform work. Select individuals require TS/SCI clearance and they are identified in the tables in Section 4.3 Key Personnel, paragraph 4.3.1 and 4.3.2.

5.1.2 Sensitive Information is defined in the DHS Instruction Handbook, 121-01-007, "The Department of Homeland Security, Personnel Security, Suitability and Fitness Program" as "Any information, the loss, misuse, disclosure, unauthorized access to, or modification of, which could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria by an Executive Order or an Act of Congress to be kept secret in the interests of national defense, homeland security, or foreign policy. This definition includes one of the following categories of information:

A. Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. section 21 1-224; its implementing regulations, 6 C.F.R. Part 29; or the applicable PCII Procedures Manual; or

B. Sensitive Security Information (SSI), as described in 49 C.F.R. Part 1520; or

C. Sensitive but Unclassified Information (SBU) -For Official Use Only -, which consists of any other information which:
   (1)If provided by the government to the contractor, is marked in such a way to place a reasonable person on notice of its sensitive nature;
   (2) Is designated "sensitive" in accordance with subsequently adopted homeland security information handling requirements."

5.1.3 Contract Company must obtain and retain an active Top Secret facility security clearance (FCL) and Safeguarding Level as None granted by the Defense Counterintelligence and Security Agency (DCSA) at the time of solicitation/proposal submission. DHS does not accept interim FCLs. Contractor will not be required to receive and/or store classified information at their facility.

5.1.4 Contract personnel requiring Top Secret access and eligibility/access to Sensitive Compartmented Information (SCI) are required to obtain and retain the appropriate PCL and level of access while providing contract support to exceed the terms of the contract. All other contract personnel require access to unclassified sensitive (see table 4.3.1 & 4.3.2).

5.2 POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDER

5.2.1 The procedures outlined below shall be followed for the DHS CISA Personnel Security Division (PSD) to process background investigations, Entry on Duty determinations, and Fitness determinations, as required, in a timely and efficient manner.

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

5.2.3 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 submit the below completed forms to the CISA/PSD. The Standard Form (SF) 85-P must be completed electronically through the Office of Personnel Management's e-QIP SYSTEM. The SF-85P signature pages and other completed forms must be given to the OSCO/PSD no less than thirty (30) 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:

1) Standard Form (SF) 85-P, —Questionnaire for Public Trust Positions
2) SF-85P Certification
3) SF-85P Authorization for Release of Information
4) FD Form 258, —Fingerprint Card (2 copies)
5) DHS Form 11000-6 —Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement
6) DHS Form 11000-9, —Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act
7) Only complete packages will be accepted by the DHS OCSO/PSD. Specific instructions on submission of packages will be provided upon award of the contract.

5.2.4 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.

5.2.5 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 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 meeting / transition attendances to prepare for the new contract.

5.2.6 The CISA/PSD shall be notified of all terminations/resignations within five days of occurrence. The Contractor shall return to the Contracting Officer's 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 whom it was issued and the last known location and disposition of the pass or card.

5.3 PERIOD OF PERFORMANCE

Period of Performance	Date
Base Year	09/30/2024 – 09/29/2025
Option One	09/30/2025 – 09/29/2026
Option Two	09/30/2026 – 09/29/2027

5.4 PLACE OF PERFORMANCE

5.4.1 The place of performance will be a combination of telework at the Contractor personnel residence when telework is authorized and at the CISA offices listed below. .

5.4.2 DHS Facility Locations
TS/SCI information will be accessed at 4601 Fairfax Drive, Arlington, VA 22201 and 1110 N Glebe Road, Arlington, VA 22201. TS/SCI information will only be accessed at these two Government locations. Unclassified Sensitive information will be accessed at 4200 Wilson Boulevard, Arlington, VA 22203.

5.4.3 Contractor Facility Location No work will be performed at contractor facility location.

5.5 Contractor Telework/Remote Personal Residence Work Locations

5.5.1 Teleworking for federal government contractors will be considered on a situational basis to the extent practicable to meet DHS mission needs. Teleworking allows contractor personnel to perform their contractual requirements outside of the designated CISA office locations, typically at a contractor's personal residence or a corporate telecommuting office location. Telework for contractor personnel provides the government flexibility to meet unique CISA organizational and facility needs and requirements. The goal of teleworking for Contractor personnel is to enhance the delivery of services that support the DHS mission. Teleworking is permitted under the task order in accordance with the requirements below. All work performed outside of the identified Contractor and or Government facilities will be performed at the Unclassified FOUO level and ensuring access to personnel who are authorized access.

5.5.2 Additionally, the provision to permit contractor telecommuting may be revoked at the task order level at any time if the Government makes such determination. The telecommuting provision does not change any task order requirements; all other terms and conditions of the task order remain in full force and effect.

5.5.3 The Contractor shall charge the same applicable fixed hourly rate as for a Government site for those Contractor personnel when they telecommute at their designated telecommuting location.

5.6 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 0800 and 1700EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including

weekends and holidays, to fulfill requirements under this SOW. Additionally, the Contractor may be required to support 24X7 coverage during normal operations and in response to CISA's enhanced operations due to a major cyber event or significant cyber incident.

5.7 TRAVEL

Contractor travel shall not be required for this requirement.

5.8 Business Continuity Plan

5.8.1 The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 30 business days after the date of award and will be updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

1) A description of the Contractor's emergency management procedures and policy.
2) A description of how the Contractor will account for their employees during an emergency.
3) How the Contractor will communicate with the Government during emergencies.
4) A list of primary and alternate Contractor points of contact, each with primary and alternate:
    a. Telephone numbers
    b. E-mail addresses

5.8.2 Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational as soon as possible or as directed by the Government, and shall be sustainable until the emergency situation is resolved, and normal conditions are restored or the task order is terminated, whichever comes first. In case of a life-threatening emergency, the COR shall immediately contact the Contractor Program Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occurs, the Contractor Program Manager and the COR shall promptly open an effective means of communication and verify:

1) Key points of contact (Government and Contractor)
2) Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
3) Means of communication available under the circumstances (e.g., email, webmail, telephone, FAX, courier, etc.)
4) Essential Contractor work products expected to be continued by priority.

5.8.3 The Government and Contractor Program Manager shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. Contractors shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

5.8.4 Due to the sensitive nature of the work to be performed under this contract, Contractor personnel awarded under this SOW are considered essential personnel and are required to report to work during any period of Government shutdown unless otherwise directed by the Partnership

Branch Chief.

5.9 Progress Reports

The Program Manager shall provide weekly report that includes a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

5.10 Progress Meetings

The Contractor PM shall be available to meet with the COR and PM upon request to present deliverables, discuss progress, exchange information, and resolve emergent technical problems and issues. The meetings shall take place with the COR, JCDC Partnerships Branch Chief, JCDC Partnerships Deputy Branch Chief, PM, and Government Task Managers at the Government's facility or virtually as determined by the government.

5.11 General Report Requirements

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows XP and Microsoft Office Applications).

5.12 Protection of Information

5.12.1 Contractor access to proprietary information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with HSAR 3052.204-72, Safeguarding of Controlled Unclassified Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

5.12.2 The Contractor shall use Government furnished information, data, and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data, and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data, and documents to outside parties without the prior and explicit consent of the Contracting Officer.

6.0 GOVERNMENT FURNISHED RESOURCES

6.1 The Government will provide the workspace, equipment and supplies necessary to perform the onsite portion of Contractor services required in this task order. Contractor staff who do not interface with DHS systems will not require Government Furnished Equipment (GFE). The Government will provide equipment for off-site Contractor use in performing work under this task order.

6.2 The Contractor shall use Government furnished facilities, property, equipment and supplies only for the performance of work under this task order and shall be responsible for returning all Government furnished facilities, property, and equipment in good working condition, subject to normal wear and tear. The Contractor shall keep and maintain an inventory of GFE, which shall be made available to the COR upon request.

6.3 Property Inventory

The Contractor shall ensure personnel apply a DHS-supplied barcode to all property purchased for CISA. Contractor/Servicing Agency must establish and maintain an accurate master inventory of all property purchase for CISA under this Contract.

6.4 Notification of Property Receipt

6.4.1 The Contractor shall confirm receipt of CISA property purchased under this SOW with the assigned CISA Accountable Property Officer (APO) and COR within five business days of receipt.

6.4.2 Monthly Asset Management Report - Contractor shall prepare a monthly Asset Management Report, which contains accurate information for all CISA property located at their facility. At a minimum, this report shall include:

a. DHS Barcode
b. Acquisition Date
c. Acquisition Status
d. Asset Condition
e. Manufacturer Name
f. Manufacturer Model
g. Asset Description
h. Serial Number
i. Asset Cost
j. Location

6.4.3 Invoice/Receipts - Contractor shall ensure copies of all invoices/packing slips/receipts for property purchased for CISA accompanies the Monthly Asset Management Report.

7.0 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment, and services necessary to fulfill the requirements of this task orders, except for the Government Furnished Resources specified in SOW 6.0.

8.0 RECORDS MANAGEMENT OBLIGATIONS

8.1 Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

8.2 In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

8.3 In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for

Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

8.4 CISA and its Contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of CISA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to CISA. The Agency must report promptly to NARA in accordance with 36 CFR 1230.

8.5 The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the task order. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to CISA control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the task order. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

8.6 The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and CISA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

8.7 The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with CISA policy.

8.8 The Contractor shall not create or maintain any records containing any non-public CISA information that are not specifically tied to or authorized by the contract.

8.9 The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

8.10 CISA owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which CISA shall

have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

8.11 Training - All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take CISA-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

8.12 Flow-down of requirements to subcontractors - The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this, and require written subcontractor acknowledgment of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

9.0 ACRONYMS LIST

C
CISA – Cybersecurity and Infrastructure Security Agency CIPAC – Critical Infrastructure Protection Advisory Council CO – Contracting Officer
COI – Communities of Interest COOP – Continuity of Operations
COR – Contracting Officer's Representative CSD – Cybersecurity Division

D
DHS – Department of Homeland Security
F
FAQ – Frequently Asked Questions FCRA – Fair Credit Reporting Act FOUO – For Official Use Only

G
GFP – Government Furnished Property

H
HSAR – Homeland Security Acquisition Regulation HSIN – Homeland Security Information Network

I
ICS-CERT – Industrial Control Systems Cyber Emergency Response Team ICSJWG – Industrial Control Systems Joint Working Group
IT – Information Technology

L
LNO – Liaison Officers

N
NCAS – National Cyber Awareness System
NCCIC – National Cybersecurity and Communications Integration Center

O
OC – Operational Collaboration
OSA – Office of Special Acquisitions

P
PCII – Protected Critical Infrastructure Information PII – Personally Identifiable Information
PM – Program Manager
PMR – Program Management Review

R
RFA – Request for Access

S
SCI – Sensitive Compartmented Information
SCIF – Sensitive Compartmented Information Facility SLTT – State, Local, Tribal, Territorial
SME – Subject Matter Expert
SOP – Standard Operating Procedures SOW – Statement of Work
SSO – Special Security Officer

T
TS – Top Secret
TTP – Tactics, Techniques, and Procedures

U
U – Unclassified

10.0 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 HLS EA.
- 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 Reference Model and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards will comply with 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 be in 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.

10.1 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:

- All data built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Data Reference Model.
- All software built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Technical Reference Model.

10.2 EPEAT AND ENERGY STAR LANGUAGE

"All hardware procured directly or in support of this action must meet applicable and appropriate Electronic Product Environmental Assessment Tool (EPEAT) and ENERGY Star standards."