ELECTRIC VEHICLE CHARGING STATION MAINTENANCE PERFORMANCE WORK STATEMENT

1. BACKGROUND:

The Defense Logistics Agency (DLA) must maintain a serviceable charging or refueling infrastructure for Zero Emission Vehicles (ZEVs) or Plug-in Hybrid Electric Vehicles (PHEVs). DLA currently has 10 operational electric vehicle charging stations located at:

- (2) Fort Belvoir, VA
- (I) Richmond, VA
- (2) Tracy, CA
- (2) Philadelphia, PA
- (2) New Cumberland, PA*
- (I) Columbus, OH

*6 Additional chargers scheduled to be added during 2026

2. OBJECTIVE:

The government intends to award a task order against a Federal Supply Schedule (FSS) contract to cover maintenance of currently installed vehicle charging stations.

3. SCOPE:

This requirement is for one base year and four option years of a network service plan subscription, Charge Point CT4000-ASSURE1 maintenance warranty coverage, and required cybersecurity compliance. Only ChargePoint or ChargePoint-approved O&M Partners can perform maintenance/ warranty work on ChargePoint EV charging stations. DLA intends to purchase:

CT4000-ASSURE1, CT4000 Family Assure Plan - 1 Year, manufacturer - ChargePoint. I yr Prepaid Assure Plan - Assure is the most comprehensive parts and on- site labor warranty. Parts and On-Site Labor to repair or replace any manufacturing defect and includes station management, remote monitoring of station and proactive repair dispatch. A successful Site Validation is required to activate any ChargePoint Assure product. Assure is priced per station.

Vendor shall also provide a network service plan to include station management, remote monitoring of the station and proactive repair dispatch. The remote monitoring offered by the Vendor must include end-user instructions that address how to:

- Establish an account (specify driver versus station owner differences). The vendor shall outline what the account being established is, what type of information is being stored, and where the information will be stored.
- Establish an account (specify driver versus station owner differences).
- Establish levels of network visibility/access within the user's fleet organization.
- Limit system access to authorized users and processes acting on behalf of authorized users, and devices (including other systems).
- Limit system access to the types of transactions and functions that authorized users are permitted to execute.
- Track energy usage by user; and
- Monitor other performance metrics via an online dashboard developed and supported by the vendor. The vendor shall provide the information on the dashboard prior to implementation and seek approval for use from the COR.

The Vender must notify the customer agency's Ordering Contracting Officer and Contracting Officer's Representative, in writing, at least 60 days prior to expiration of network service plans. The notification must include, at a minimum:

- EVSE Identifier Information.
- Location of the EVSE (city and state).
- Order Number under which the network services are currently being provided; and
- Last day of service for each station.

Maintenance must be performed by ChargePoint certified technicians. Service support response is required within one business day. For repairs requiring parts to be ordered, technicians will be on-site to repair stations within one day of receiving any required parts. The maintenance warranty will include both maintenance, parts, and labor. The warranty will cover repair of any type of equipment failure or any kind of damage including damage caused by accidents, vandalism, and excessive wear and tear.

4. PRODUCTS:

Contract Line Item Number	Period of Performance	Description	Quantity
0001	Sept 30, 2026 - Sept 29, 2027	EVSE Maintenance Plan	10
0002	Sept 30, 2026 - Sept 29, 2027	Network Service Plan	16
0003	Sept 30, 2026 - Sept 29, 2027	Cyber Security (Not to exceed)	
1001	Sept 30, 2027 - Sept 29, 2028	EVSE Maintenance Plan	16
1002	Sept 30, 2027 - Sept 29, 2028	Network Service Plan	27
1003	Sept 30, 2027 - Sept 29, 2028	Cyber Security (Not to exceed)	
2001	Sept 30, 2028 - Sept 29, 2029	EVSE Maintenance Plan	16
2002	Sept 30, 2028 - Sept 29, 2029	Network Service Plan	27
2003	Sept 30, 2028 - Sept 29, 2029	Cyber Security (Not to exceed)	
3001	Sept 30, 2029 – Sept 29, 2030	EVSE Maintenance Plan	16
3002	Sept 30, 2029 – Sept 29, 2030	Network Service Plan	27
3003	Sept 30, 2029 – Sept 29, 2030	Cyber Security (Not to exceed)	
4001	Sept 30, 2030 – Sept 29, 2031	EVSE Maintenance Plan	16
4002	Sept 30, 2030 – Sept 29, 2031	Network Service Plan	27
4003	Sept 30, 2030 – Sept 29, 2031	Cyber Security (Not to exceed)	

5. PLACE OF PERFORMANCE:

a. Location I: 8725 John J. Kingman Rd, Ft Belvoir, VA 22060
b. Location 2: 3990 E. Broad Street, Columbus, OH 43213
c. Location 3: 6090 Strathmore Rd, Richmond, VA 23237
d. Location 4: 25600 S. Chrisman Rd, Tracy, CA 95304
e. Location 5: 5730 3rd Street, Bldg. 750, New Cumberland, PA 17070
f. Location 6: 700 Robins Avenue, Philadelphia, PA 19111
g. Current covered stations include the following (Government Furnished Property):

i. **Stations at Ft Belvoir, VA (2):**

2 charging stations – completed December 20, 2017
Description: Fleet, Level 2, Gateway, Pedestal/Bollard Mount, Dual Port Manufacturer: ChargePoint
Manufacturer Part Number: CT402 l-GWN-1
CT4000-ASSURE1 - current maintenance coverage expires September 29, 2026

ii. **Stations at Tracy, CA (2):**

2 charging stations - 1 dual port, 1 single port

Station 1: operational validation completed 04/17/2018
Description: Fleet, Level 2, Gateway, Pedestal/Bollard Mount, Dual Port
Manufacturer: ChargePoint
Manufacturer Part Number: CT4021-GWN-1
CT4000-ASSURE1 - current maintenance coverage expires September 29, 2026

Station 2: operational validation completed 04/17/2018
Description: Fleet, Level 2, Gateway, Pedestal Mount, Single Port
Manufacturer: ChargePoint
Manufacturer Part Number: CT4011-GWN-1
CT4000-ASSURE1 - current maintenance coverage expires September 29, 2026

iii. **Station at Richmond, VA (1):**

1 Charging Station operational validation completed 03/15/2018
Description: Fleet, Level 2, Gateway, Pedestal/Bollard Mount, Dual Port
Manufacturer: ChargePoint
Manufacturer Part Number: CT4021-GWN-1
CT4000-ASSURE1 - current maintenance coverage expires September 29, 2026

iv. **Stations at Philadelphia, PA (2):**

Station 1: operational validation completed 04/17/2018
Description: Fleet, Level 2, Gateway, Pedestal/Bollard Mount, Dual Port
Manufacturer: ChargePoint
Manufacturer Part Number: CT402l-GWN- 1
CT4000- ASSURE1 - current maintenance coverage expires September 29, 2026

Station 2: operational validation completed 04/17/2018
Description: Fleet, Level 2, Gateway, Pedestal/Bollard Mount, Single Port
Manufacturer: ChargePoint

Manufacturer Part Number: CT4011-GWN- 1
CT4000- ASSURE1 - current maintenance coverage expires September 29, 2026

v. **Stations at New Cumberland, PA (2): *6 stations expected to be added in 2026 and will be included under a mod for that option period that the warranty ends.**

Station 1: operational validation completed 04/17/2018
Description: Fleet, Level 2, Gateway, Pedestal Mount, Single Port
Manufacturer: ChargePoint
Manufacturer Part Number: CT4011-GWN-1
CT4000- ASSURE1 - current maintenance coverage expires September 29, 2026

Station 2: operational validation completed 04/17/2018
Description: Fleet, Level 2, Gateway, Pedestal Mount, Single Port
Manufacturer: ChargePoint
Manufacturer Part Number: CT4011-GWN-1
CT4000-ASSURE1 - current maintenance coverage expires September 29, 2026

*Station 3: operational validation completed - TBD
Description: Fleet, Level 2, Gateway, Pedestal Mount, Dual Port
Manufacturer: ChargePoint
Manufacturer Part Number: pending CT4021-GWN-1
CT4000-ASSURE1 - current warranty coverage expected t o expire 2027

*Station 4: operational validation completed - TBD
Description: Fleet, Level 2, Gateway, Pedestal Mount, Dual Port
Manufacturer: ChargePoint
Manufacturer Part Number: pending CT4021-GWN-1
CT4000-ASSURE1 - current warranty coverage expected t o expire 2027

*Station 5: operational validation completed - TBD
Description: Fleet, Level 2, Gateway, Pedestal Mount, Dual Port
Manufacturer: ChargePoint
Manufacturer Part Number: pending CT4021-GWN-1
CT4000-ASSURE1 - current warranty coverage expected t o expire 2027

*Station 6: operational validation completed - TBD
Description: Fleet, Level 2, Gateway, Pedestal Mount, Dual Port
Manufacturer: ChargePoint
Manufacturer Part Number: pending CT4021-GWN-1

CT4000-ASSURE1 - current warranty coverage expected to expire 2027

*Station 7: operational validation completed - TBD
Description: Fleet, Level 2, Gateway, Pedestal Mount, Dual Port
Manufacturer: ChargePoint
Manufacturer Part Number: pending CT4021-GWN-1
CT4000-ASSURE1 - current warranty coverage expected to expire 2027

*Station 8: operational validation completed - TBD
Description: Fleet, Level 2, Gateway, Pedestal Mount, Single Port
Manufacturer: ChargePoint
Manufacturer Part Number: pending CT4011-GWN-1
CT4000-ASSURE1 - current warranty coverage expected to expire 2027

vi. **Station at Columbus, OH (1):**
1 Charging Station operational validation completed 9/20/2018
Description: Fleet Level 2, Gateway. Pedestal Mount, Dual Port
Manufacturer: ChargePoint
Manufacturer Part Number: CT402l-GWN- 1
CT4000-ASSURE1 - current maintenance coverage expires September 29, 2026

6. PERIOD OF PERFORMANCE:

Base Year:	September 30, 2026 - September 29, 2027
Option Year 1:	September 30, 2027 - September 29, 2028
Option Year 2:	September 30, 2028 - September 29, 2029
Option Year 3:	September 30, 2029 - September 29, 2030
Option Year 4:	September 30, 2030 - September 29, 2031

7. CYBER LANGUAGE

The contractor shall provide cybersecurity (CS) in accordance with all current policies, procedures, and statutes.

7.1 Personnel Requirements

The Contractor shall provide skilled, experienced, professional and/or technical personnel consistent with the task requirements of this PWS. Contractor personnel supporting cybersecurity functions shall be appropriately certified, educated or have experience according to DoW Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program upon contract and/or MOD awards.

The Contractor is responsible to provide qualified personnel, as specified, and as required by the PWS, and shall bear all cost for training its personnel. The Government will not reimburse the Contractor for the cost for training Contractor personnel. Training will not be allowed on Government time.

The Contractor shall provide a monthly DoD 8140.03 deliverable report as specified by the COR/TPOC, that includes a list of applicable key personnel. The following information shall be provided in the report, due by the 5th business day of each month:

Work Role
Work Role Task
Company
Contract Name/Description
COR Name
Contract #
The Contractor will Identify the Certification, Work Experience or Training that meets the DoD 8140.03 related to the EVSE.

If a certification identified in the DoD 8140.03 report becomes obsolete during the life of the contract, the Contractor shall be responsible for ensuring applicable personnel obtain an acceptable replacement certification prior to the IT/OT product's end of support or end of life.

The provisions of this PWS shall be fully applicable to all subcontractors.

Information given to the Contractor during the life of this contract shall only be used for the purpose of carrying out the provisions of this contract. Agency marked "Controlled Unclassified (CUI)" or bearing other sensitivity markings shall be handled in accordance with (IAW) Agency information security program regulations and shall not be divulged or disclosed without Agency permission in writing. Requests for disclosure shall be addressed to the Contracting Officer (KO).

7.1.2 Citizenship

Each Contractor employee shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence, or who presents evidence from the Immigration and Naturalization Service that employment will not affect his immigration status.

7.2 Cybersecurity Strength Requirements

The Contractor shall satisfy the Risk Management Framework (RMF) requirements of subchapter III of chapter 35 of Title 44, United States Code (U.S.C.), also known as the "Federal Information Security Management Act (FISMA) of 2002 (Modernization 2014)".

The Contractor shall enable DLA to meet the standards required by the Office of Management and Budget (OMB) and the Secretary of Commerce, pursuant to FISMA and section 11331 of Title 40, U.S.C.

FIPS 199 / CNSSI 1253 Security Categorization: The Contractor shall participate in categorization discussions with the DLA J6 PM, functional lead, and the Information System Security Manager (ISSM) and provide all required FIPS 199 documentation as requested to support security categorization.

The Contractor shall collaborate with the Government Program Manager on system categorization based on sound technical expertise in accordance with FIPS 199 then work in coordination with the prescribed DLA System Owner (SO) and ISSM to support the categorization IAW FIPS 199, CNSSI 1253 and Office of the Secretary of War (OSW) Facility Related Control Systems (FRCS) Master List including DLA specific systems, then document the results of the security categorization in the System DLA FIPS 199 document and the Concept of Operations (CONOPs).

Assigned DLA J6 PM will coordinate with the Contractor to identify and document Confidentiality, Availability, Integrity (CIA) of the system in a DLA FIPS 199 document for approval by DLA ISSM personnel.

7.3 Cybersecurity Assurance Requirements

At a minimum, the solution must meet Impact Level IL2 in FedRamp.

Typical Contractor services activities include:

a) Defining how the DLA FRCS Automation Solution will connect to external (e.g., plant) and networks, by system description, concept, hardware and software lists, and dataflow diagrams.
b) Gaining approval of the DLA asset owner for many of the decisions made and outputs generated during the execution of these activities.

The Contractor shall design, develop, and integrate cybersecurity solutions supporting the Department of War and all other applicable Government agencies.

This will be achieved through abiding by all applicable cybersecurity policies, regulations, and directives to ensure a favorable Assessment and Incorporate (A&I), as well as obtaining an Authority to Connect (ATC) to DLA's network. The Contractor shall mitigate risk identified through the RMF authorization process down to a level acceptable to the DLA Authorizing Official (AO).

The solution shall comply with the security control requirements documented in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53r5, "Security and Privacy Controls for Federal Information Systems and Organizations" and NIST 800-82r3, "Guide to Industrial Control Systems (ICS) Security". The Contractor shall provide details of any alternative, but equally effective security measures used to compensate for the inability to satisfy a particular derived security requirement (mitigation to control compliance findings). This information shall be submitted in writing to the DLA J6 PM for cybersecurity approval as soon as the alternative is identified. All vulnerabilities associated with solutions must be reported to the DLA J6 PM with a Plan of Action and Milestones (POA&M) for remediation.

7.4 Tasks and Deliverables

The Contractor shall provide required implementation and design documentation to the DLA J6 PM and security engineering teams to conduct a cybersecurity risk assessment (RA) of solution. Results from accepted RAs will be incorporated into the Systems concepts of operations (CONOPs).

The Contractor, in collaboration with assigned security manager, DLA J6 PM and system owner, shall identify and document applicable cybersecurity enterprise architectures and deliver system conceptual design drawings.

The full list of deliverables is listed in Section 7.7 Deliverables.

The Contractor shall leverage, to the greatest extent possible, DLA Enterprise processes and capabilities.

7.5 Information and Operational Technology Infrastructure Requirements

The Contractor will be responsible for the implementation including meeting all applicable STIG compliance.

The Contractor shall be responsible for all configuration and deployment which meet DoW, NIST and USG regulatory and cybersecurity policy requirements.

Any OT solution(s) and/or system(s) with IT Infrastructure provided by the Contractor must be upgradeable and remain compliant to cybersecurity specifications during the lifecycle of the solution. Contractor supplied systems must meet DoW STIG requirements, with any exceptions noted in the design documentation.

The Contractor is responsible for all software maintenance activities for any/all appliances including but not limited to, firmware updates, OS patching, software patches and documentation, etc. for the duration of the contract period.
The Contractor will be responsible for all physical maintenance activities for any/all appliances including but not limited to, replacement of defective components such as hard drives (to be destroyed onsite per DoW policy, guidance), motherboards, daughterboards etc. for the duration of the contract period.

Activities are typically short and frequently recurring, and may include one or more of the following:

a. Equipment upgrades and maintenance, including small engineering adjustments not directly related to control algorithms
b. Component and system migration
c. Change management
d. Contingency plan management

System(s) shall operate using a Contractor fully supported operating system (OS), software, and firmware throughout the duration of the contract. All operating systems, software, and firmware shall be upgraded prior to the Contractor's end of mainstream support for the operating system, software, or firmware. The solution must be upgradeable and remain compliant with DoW cybersecurity specifications during the lifecycle of the solution.

7.6 Kick off Meeting, Progress Meetings and Status Reports

The Contractor shall provide a Points of Contact (POC) List within 1 business day of contract award.

The Contractor shall attend any post award conferences convened by the contracting activity IAW Federal Acquisition Regulation Subpart 42.5, Post Award Orientation, to discuss and develop mutual understandings/standards of contract performance requirements.

The Contractor shall coordinate a Kick-Off Meeting within a week after contract award. The meeting shall include all necessary personnel from both the Government and Contractor to achieve a clear and mutual understanding of all requirements. The Contractor shall provide written meeting minutes to the COR within two (2) days after the meeting. Meeting minutes shall include a list of all action items, the party responsible for each item, and the agreed-upon due date. The status of all open action items will be

the first topic of discussion at the subsequent meeting. The Contractor is responsible for all meeting logistics, including scheduling, providing conference facilities or virtual meeting links, and distributing all relevant materials. The Contractor shall provide a draft agenda to the COR for review and approval no later than three (3) business days prior to any scheduled meeting.

The Contractor's Project Manager shall be required to schedule with the COR and subcontractors to discuss contract performance during Periodic Progress Meetings. The frequency of these meetings shall be determined by the COR. These meetings may cover but are not limited to discussions on maintenance plans, cyber progress, and issues/ concerns. The Contractor shall provide written meeting minutes to the COR within two (2) days after the meeting. Meeting minutes shall include a list of all action items, the party responsible for each item, and the agreed-upon due date. The status of all open action items will be the first topic of discussion at the subsequent meeting. The Contractor is responsible for all meeting logistics, including scheduling, providing conference facilities or virtual meeting links, and distributing all relevant materials. The Contractor shall provide a draft agenda to the COR for review and approval no later than three (3) business days prior to any scheduled meeting.

A Monthly Status Report must be submitted by the 5th business day of each month, detailing all activities from the previous calendar month. It should include a detailed summary of all tasks completed for the month, a transparent account of any issues encountered and their resolution, and a forward-look at activities planned for the upcoming month.

7.7 Deliverables

Within 30 calendar days of contract award/modification, the Contractor shall deliver a comprehensive Cybersecurity Risk Management Framework (RMF) Artifacts Deliverables Schedule to the Government for written approval. This schedule must include detailed timelines and specific delivery dates for all required cybersecurity RMF artifacts, explicitly identifying milestones for both draft and final versions of each document. The Government shall have 10 business days to review and approve the proposed schedule, and no work shall commence until such approval is granted in writing. Any subsequent modifications to the approved schedule require formal written submission and approval by the Government. For the cybersecurity assessment, the vendor will need to develop RMF documentation for the existing 10 charging stations and those stations identified in Section 5 that will be added in 2026.

The Government may require contractor input to the documents in the bulleted list below for an A&I. If so, the Government will provide the necessary templates:

- Configuration Control Working Group Charter
- Supplemental Implementation Guide Contingency Plan
- MOU/MOA/SLA
- Incident Response Plan
- Maintenance SOP
- Privacy Documentation
- System Development Life Cycle (SDLC) Documentation
- DLA Access Control Policy
- Disaster Recovery Plan

The contractor will provide the documents in the table below. The Government will provide the necessary templates, if available. If no template is available, the Government will specify required format and content for deliverable:

RMF Documentation:			
#	Deliverable Name	Reference	Submission Due
1	System Diagrams (Architecture, Authorization Boundary, Data Flow and Purdue)	7.3 Cybersecurity Assurance	Per Government approved deliverable schedule Update at least annually
2	Comprehensive Hardware/ Software List (DLA provided template at TO level)	7.3 Cybersecurity Assurance	Per Government approved deliverable schedule after contract award Update at least annually
3	System CONOPs	7.4 Tasks and Deliverables/7.2 Cybersecurity Strength Requirements	Per Government approved deliverable schedule Update at least annually
4	FIPS 199 Categorization	7.2 Cybersecurity Strength Requirements	Per Government approved deliverable schedule Update at least annually
5	Privacy Impact Assessment	7.3 Cybersecurity Assurance	Per Government approved deliverable schedule Update at least annually
6	Installation/ Configuration Documentation	7.4 Tasks and Deliverables	Per Government approved deliverable schedule Updates as required
7	Application Software release/patch Documentation	7.4 Tasks and Deliverables	Per Government approved deliverable schedule Updates as required
8	FedRAMP Authorization (if cloud technology)	7.3 Cybersecurity Assurance	Remain current at IL2

7.8 Privacy Act Information

If the vendor comes across any PII the vendor needs to notify DLA. The system has been identified as having no PII.