Appendix A - Statement of Work

STATEMENT OF WORK
for
Electric Vehicle Supply Equipment (EVSE) and Ancillary Services

1. Background

Transportation accounts for roughly 29% of U.S. greenhouse gas emissions (GHG) or approximately 6,558 million metric tons of CO2 equivalent. The federal fleet is comprised of approximately 657,500 vehicles and drove 4.2 billion miles in 2020 using approximately 371.8 million gallons of fuel[1]. This equates to 3.4 million metric tons of GHG emissions or .05% of the total amount of transportation related emissions. Although seemingly small, the federal fleet is highly visible and presents the perfect opportunity for the federal government to lead by example in reducing GHG emissions by moving to a zero-emission fleet.

To drive this effort, President Biden signed Executive Order 14008 which promotes using the federal government's buying power and real estate and asset management to develop a Federal Clean Electricity and Vehicle Procurement Strategy. The Chair of the Council on Environmental Quality, the Administrator of General Services, and the Director of the Office of Management and Budget, in coordination with the heads of other relevant agencies, are assisting the National Climate Advisor in developing a comprehensive plan to create jobs and stimulate clean energy industries by revitalizing the federal government's sustainability and climate resilience efforts. The plan's aim is to use all available procurement authorities to achieve or facilitate clean and zero-emission vehicles (ZEV) for Federal, State, local and Tribal government fleets, including vehicles of the United States Postal Service.

As the mandatory source for executive agencies purchasing non-tactical vehicles in the United States, the General Services Administration (GSA) Office of Fleet Management has a significant role to play in the Biden Administration's initiative to electrify the federal fleet through its procurement of ZEVs and associated charging infrastructure.

2. Purpose

The purpose of this acquisition is to establish multiple governmentwide Blanket Purchase Agreements (BPA) that will provide a streamlined procurement process for eligible ordering activities to purchase electric vehicle supply equipment (EVSE) and ancillary services and deploy charging infrastructure. These BPAs are intended to offer a broad portfolio of electric vehicle recharging stations and ancillary services to support eligible ordering activity needs as the fleet transitions to electric vehicles.

3. Scope

[1] Annual Federal Fleet Report (2020) https://www.gsa.gov/policy-regulations/policy/vehicle-management-policy/federal-fleet-report

The scope of this acquisition encompasses EVSE infrastructure solutions such as charging hardware, charging as a service, site planning, and other related solutions and ancillary services. Any EVSE product or ancillary services offered must comply with the applicable requirements described within this Statement of Work.

3.1 Overarching Objectives

Our objective is to leverage the government's buying power for electric vehicle charging station infrastructure needs and streamline purchasing for a wide array of offerings to meet GSA's customer needs. The overarching objectives are to make the following products and services available under the BPAs:

- a full range of charging infrastructure solutions for governmentwide use;
- a broad hardware portfolio such as bollard, pedestal, solar, V2G, distributed and integrated energy storage solutions and portable charging solutions;
- non-ownership charging options such as Charging as a Service;
- an array of ancillary services such as EVSE site assessments and make-ready services, network data plans, smart metering, power management and distributed energy software, extended warranty; and operation and maintenance plans;
- geographic availability in the continental United States, Alaska, Hawaii, and other U.S. territories as well as in Europe;
- onboarding of emerging infrastructure technology throughout the duration of the BPA; and
- quarterly reports on products and services sold under the BPA.

4. EVSE Requirements

The price for each configuration offered must include the unit and all mounting hardware required to support the unit, 12 months of service (for networked stations) as well as the cost of commissioning or activation, and configuration assistance with user account set-up.

EVSE configurations offered may be:

- Commercial grade.
- Offered as an equipment purchase or as "Charging as a Service" (charge per port) model in which station is leased.

The following are minimum technical specification requirements for EVSE:

Power:	**Level 1 EVSE** - Must supply an average power output of 1.2 kW to 1.9 kW. **Level 2 EVSE** - AC power output. Must supply an average power output of 6.6 kW to 19.2 kW. **DC Fast Charging EVSE** - DC power output. Must supply an average power output greater than 22 kW. **Solar/Off-grid EVSE -** Must be capable of powering a level 1, level 2, or DC fast charger as stated in the corresponding level requirements. **Portable EVSE** - Must be capable of generating equivalent power output of level 1, level 2, or DC fast charger. Must be capable of transporting in a vehicle and storing energy for later use to power an electric vehicle.

Network:	• Non-networked or Network-capable (cellular with option for ethernet connection/cell repeater in locations without cellular service only). • If networked, options must include 1 year of data service (standard), 3 years or 5 years.
Mount:	Must be free standing or self-contained (e.g., Pedestal, Wall).
Port:	Single or multi-port
Safety:	Must meet all safety and compliance standards including UL 2202, UL 2251, UL 2594, NFPA, IEC, CSA, NEC, SAE, and other regional standards where applicable.
Energy Star:	Level 2 EVSE must be ENERGY STAR certified or offeror must provide full reasoning and information of the system efficiency, as to why the units are not ENERGY STAR certified. **https://www.energystar.gov/productfinder/product/certified-evse/results** (ENERGY STAR requirement for DC fast chargers may be included at a later date).

4.1 Other Charging Types/Non-conventional

GSA will also consider non-conventional charging infrastructure options. For example, high power wireless charging, battery storage, battery swapping or any emerging technology which involves the recharging of electric vehicles.

5. Ancillary Services

5.1 Metering or Load/Energy Management Technology

To support fleet operations and optimize electric vehicle utilization the Government requires Energy Management Equipment (UL 916 certified) or "smart" metering, to include load management or the ability to optimize charging patterns to minimize fixed, up-front costs and variable long-term costs, to include energy and site upgrades. Smart metering:

- can allow for the sharing of existing power among multiple stations to help to achieve the maximum aggregate electrical load for each group of stations.
- can work in tandem with or independently of the EVSE software and can manage demand and potentially help sites avoid costly upgrades and reduce utility charges by flattening out demand peaks.
- provides the ability to assign a group of stations a peak power limit.

5.2 EVSE Site Planning, Make-Ready and other related services

EVSE site assessment and planning services may be provided in conjunction with the purchase of an EVSE charging station if not already included with the EVSE purchase. EVSE assembly, permitting services and “make-ready” EVSE services may also be provided. Make-ready charging station solutions may encompass multi-step services or processes to prepare an EVSE for installation. These types of services may include but are not limited to:

- Consulting services;
- EVSE site assessment;
- Permitting/inspection (as applicable);
- Utility coordination;
- Site preparation (when no construction work is required);
- Affixing or securing the station;

- Basic assembly/make-ready (when no construction work is required);
- Activation; and
- Compliance assistance with local, state, and federal building codes practices and regulations.

An EVSE site assessment includes determining the electrical capacity of the site, determining location of distribution or service lines and the required power supply for the type and quantity of charging stations, risks to potential sites from the impacts of climate change, and helping to determine the best location for the installation if the customer-selected location is not ideal and the lowest cost spot.

Basic assembly/make-ready under this BPA is a commercial service as defined under FAR Part 2. It is not intended for installations requiring construction or complex alteration to real property that are subject to FAR Part 36 Construction and Architect-Engineer Contracts. If during the site assessment the need for construction or complex alterations to real property are discovered, the BPA Holder must notify the Ordering Contracting Officer so that installation services can be acquired outside of this BPA. GSA's Public Buildings Service (PBS) will issue separate IDIQs to support installation services.

5.3 Network Plan & Data Package

If providing a networked station, the price of the station must include one year of network services. Network plans may be offered for extended periods (e.g., 1, 3, 5 years) with initial purchase of EVSE or may be offered separately as a stand-alone purchase for other equipment purchased outside of the BPA.

The network plan offered by the BPA Holder must include end-user instructions that address how to:

- Establish an account (specify driver versus station owner differences);
- Pay for use;
- Collect Payment;
- 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 BPA Holder.

5.3.1 Network Service Plan Notification

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

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

5.4 Operation and Maintenance Plan

The Operation and Maintenance Plan is intended to mitigate charging station repair issues before they

happen and detect issues when they happen more quickly. If offered, the plan must include the following:

- Statement on value proposition or service guarantee;
- Service technician scheduled for preventative maintenance;
- Comprehensive visual, environmental, and electronic inspection of the EV Charging Station;
- Inspection of the charging connections and operational controls;
- Evaluation of system performance to ensure defined technical and environmental specifications are met;
- Verification and implementation of all required Field Advisories and Field Modifications;
- Detailed assessment of current condition and recommendation of corrective action as needed; and
- All labor and travel expenses must be included. Parts not covered under warranty will be billed at the discount offered under the BPA.

6. Other Direct Costs

Other Direct Costs (ODCs) may be included at the Order level and must be directly related and only purchased in conjunction with the supplies and services ordered under this BPA. ODCs must be an integral part of the total EVSE solution and may not be the primary purpose of the work ordered. ODC's are unknown at the time the BPA is awarded; therefore, they will be defined, priced, and awarded at the Order level. Possible ODCs may include material or equipment for installation, site preparation, etc. Travel and per diem are not considered ODCs.

7. Other Requirements

7.1 Payment / Initiation of Charge

7.1.1 Authentication

Networked EVSE must be capable of authenticating or initiating charge with Radio Frequency Identification (RFID).

7.1.2 Payment Collections and Acceptance

Fixing America's Surface Transportation Act (FAST Act)[2] authorizes the General Services Administration (GSA) and other Federal agencies to install, operate and maintain plug-in electric vehicle charging stations for privately owned electric vehicles in parking areas under the custody, control, or administrative jurisdiction of the federal agency and used by Federal employees and other authorized users, and requires the collection of fees to recover these costs. To accommodate federal employees that use EV charging stations for privately-owned vehicles where authorized, all networked Level II and DC Fast Charging stations must have capabilities to support and execute financial transactions. If there is a fee to be collected from electric vehicle owners for private use, the networked-EVSE must accept at least one major credit card and/or debit card network provider (to include Visa, MasterCard, American Express, and Discover) for payment processing and must prove to be a certified member of the Payment Card Industry

[2] Fixing America's Surface Transportation Act § 1413(c), 42 U.S.C. 6364 (2015).

(PCI) and follow Data Security Standards (DSS). Fees for private use may vary by location and agency and will be determined at the Order level.

The payment collection process may be via any of the following:

- Magnetic stripe reader
- EMV chip reader
- Contactless credit card
- RFID
- Plug and Charge or similar technologies
- Other

If an Order includes a requirement for using EV charging stations for the private vehicles of federal employees, the BPA Holder must describe in writing to the ordering activity the process for sending funds back to the agency to meet FAST Act 1413(c) requirements and provide information on additional costs, if any.

Most users for EV charging stations purchased under the BPA will be federal employees charging government-owned vehicles. Charging stations shall not require government-owned vehicle users to provide credit card or payment information to create a driver/vehicle account, or to access the charging station, or the data portal. It is preferred that the GSA SmartPay Fleet Card is accepted. To facilitate recognition of the GSA SmartPay Fleet Card, account prefixes include:

- Visa: 4486, 4614
- MC: 5563, 5565 and 5568
- WEX: 5565, 6900, 7071
- Voyager: 7088

7.2 Parts Warranty

7.2.1 Basic General Parts (1 Year)

The EVSE manufacturer's commercial warranty must be provided for all parts and components against parts failure or malfunction due to design, defective workmanship, and missing or incorrect parts, for a minimum period of 12 months from date of installation for Level 2 EVSE, DC Fast EVSE, Solar/off-grid EVSE and 12 months from the date of receipt and acceptance of the Level 1 EVSE and Portable EVSE. If the BPA Holder receives, from any supplier or subcontractor, additional overall warranty, or any component of the EVSE, including any prorated arrangements, or the BPA Holder generally extends to its commercial customers greater or extended warranty coverage, the Government must receive corresponding warranty benefits. Labor, parts, shipping cost, per diem, and travel for warranted repairs to and from the unit's installed location shall be the responsibility of the BPA Holder.

7.2.2 Advanced Warranty (optional)

Advanced warranties such as a % Uptime guarantee, accident and vandalism warranty, modem upgrades, etc. may also be offered. Warranties should be described and priced under CIN 0009 - Operation, Repair & Maintenance Plans in Attachment 4.

7.3 Operator Manuals and Training

A digital copy or link to the original equipment manufacturer (OEM) operator manual, installation manual and training materials must be furnished with each EVSE ordered.

7.4 Security, Privacy, and Supply Chain Security Requirements

Commercial Electric Vehicle (EV) Service platform providers are required to meet the appropriate Security and Privacy requirements identified in section 7.4.1 and Supply Chain Requirements in section 7.4.2 within six months of BPA award. No task orders can be issued under the BPA until the BPA Holder meets these requirements.

Offerors reselling commercial EV service platform solutions are presumed to provide EV platform provider solutions 'as-is' without additional value-added reseller systems (e.g., provisioning, billing, metering, etc.). See the ensuing sections for Security, Privacy, and Supply Chain Security Requirements.

All costs associated with meeting the Security, Privacy, and Supply Chain Security Requirements are the sole responsibility of the BPA Holder.

7.4.1 IT Security and Privacy Requirements

BPA Holders must obtain approval from GSA for the EVSE Deployment Option A or B for each distinct platform its products operate on using "NIST 171 v FedRamp Qualifying Template" (Appendix C). Products covered under Option A and B include but are not limited to network-connected charging stations or those that have the ability to connect to a network, products that store system or transactional data and network data plans.

The BPA Holder and the Government will mutually agree on a deployment option. Depending on the deployment option agreed upon, different security evaluation requirements will apply as outlined below. The final determination will be made by the Government.

OPTION A - Nonfederal Systems and Organizations - Vendor hosted (not Cloud) (Requires NIST-171)

EV network service platform provider solutions with a traditional on-prem or cloud hosted deployment model that are not delivered as a service, do not meet the NIST 800-145 cloud computing definition , and are not subject to OMB FedRAMP Policy memo FedRAMP cloud information security and privacy requirements, shall implement the security requirements below.

Option A is specific to protecting Controlled Unclassified Information in nonfederal information systems and organizations as defined in NIST 800-171 provided as a shared service not directly for or on behalf of the Government. The Nonfederal Systems and Organizations – IT Security and Privacy Requirements identified in Chapter 7 of the GSA IT Security Procedural Guide 09-48, Security Language for IT Acquisition Efforts is applicable. The BPA Holder is required to submit and receive documentation of GSA's approval as evidence of complying with the security protocols listed in Chapter 7 prior to being able to accept any orders. The BPA Holder is responsible for working with the GSA Office of the Chief Information Security Officer (CISO) to develop a system security plan, an independent assessment, and plan of Action and Milestones to be used by GSA to inform a risk-based usage consideration. This process does not result in a traditional Authorization to Operate (ATO) but does involve review - of the EV network service providers

NIST 171 package (completed at vendor cost in agreement with the above referenced GSA process guide)by the GSA CISO AND Privacy Officer for approval consideration.

GSA assumes EV network service platforms offered by most BPA Holders will be evaluated using the NIST 171 for Non-Federal Systems criteria with additional safeguards to mitigate supply chain risk. The BPA Holder shall ensure it complies with the security requirements for these types of platforms as outlined in Chapter 7 of the GSA Procedural Guide 09-48, Security Language for IT Acquisition Efforts. Please note, however, the Government will make the final determination as to whether NIST 171 is the appropriate security protocol as some solutions may require higher levels of authorization.

If in the future, the BPA Holder requests to transition from a traditional on-prem deployment model environment or a cloud deployment model that is available for use by only one client (Option A) to a public or community cloud as a service deployment model (Option B) that is subject to FedRAMP per the OMB FedRAMP policy memo requirements, the BPA Holder must pursue and achieve FedRAMP authorization in order to continue to operate. Transitioning from a Deployment Option A to a cloud as a service deployment model (Deployment Option B) is a major change and will require close coordination with the GSA, FedRAMP sponsorship, and a BPA modification to reflect the change in delivery model.

OPTION B - Nonfederal Systems and Organizations - Cloud Delivered as a Service (Requires FedRAMP)

Cloud computing offers an opportunity for the Federal Government to take advantage of cutting-edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its agencies and citizens. Established by OMB in 2011, the Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP empowers agencies to use modern cloud technologies, with emphasis on security and protection of federal information. Federal executive departments and agencies procuring commercial and non-commercial cloud services that are provided by information systems that support the operations and assets of the departments and agencies are required to ensure applicable contracts appropriately require cloud service providers (CSPs) to comply with FedRAMP security authorization requirements. This includes systems across all cloud deployment models (e.g., Public Clouds, Community Clouds, Private Clouds, and Hybrid Clouds) and all cloud service models (e.g., Infrastructure as a Service, Platform as a Service, Software as a Service) as defined per NIST 800-145, The NIST Definition of Cloud Computing.

EVSE platform provider solutions delivered as a service in the cloud, meeting NIST 800-145 cloud definition, consistent with the OMB FedRAMP Policy memo, are subject to FedRAMP cloud information security and privacy requirements.

The Cloud Information Systems – IT Security and Privacy Requirements identified in Chapter 5 of the GSA IT Security Procedural Guide 09-48, Security Language for IT Acquisition Efforts is applicable at the FIPS 199 Moderate impact level. Personally Identifiable Information (PII) is not in the scope of acquisition and PII is not expected to be stored in the BPA Holder's cloud solution.

BPA Holders are required to submit and receive documentation of GSA's approval as evidence of complying with the security protocols listed in Chapter 5 prior to being able to accept any orders.

Changes to the platform that impact the security authorization throughout the BPA's period of performance will require attendant changes to maintain the security authorization.

7.4.1.1 Vendor Requirement for Facilitating Security Validation Process

An independent assessment of the BPA Holder's documented and implemented NIST 800-171 security controls is **required**. The independent assessor must be, either by a Third-Party Assessment Organization (3PAO) or approved by the GSA OCISO, prior to selection. The BPA Holder is encouraged to also obtain 3PAO services for documentation preparation.

7.4.2 Cybersecurity-Supply Chain Risk Management Requirements (C-SCRM)

The BPA Holder must participate in GSA's C-SCRM Program including maintenance of a SCRM Plan and monitoring via third-party vendor risk illumination tools (e.g., Interos and BitSight). Please note, ordering agencies may have additional SCRM requirements at the delivery order level and will specify any additional requirements in the delivery order request. Supply chain risk requirements are below.

7.4.2.1 Cyber-Supply Chain Risk Management (C-SCRM) Plan

The BPA Holder must maintain a C-SCRM plan which identifies, if available, any relevant SCRM-related International Organization for Standardization (ISO) certifications (e.g., ISO 20243:2018, ISO 27K series, ISO 28K series). The C-SCRM plan must address the NIST 800-161 cyber supply chain security controls identified in Table 1 below. These controls are derived from NIST 800-53 Rev 5 and related to expanded supplemental guidance for mitigating supply chain risk that are complementary to the NIST 800-171 requirements for CUI.

Table 1 – NIST SP 800-53 Rev 5 Control selected for C-SCRM Plan

NIST SP 800-53 Rev 5 Control ID	NIST SP 800-53 Rev 5 Control Name
SA-4	Acquisition Process
SA-11	Developer Testing and Evaluation
SA-15	Development Process, Standards, and Tools
SA-8	Security and Privacy Engineering Principles
SI-7	Software, Firmware, and Information Integrity
SR-6	Supplier Assessments and Reviews
SR-8	Notification Agreements
SR-10	Inspection of Systems or Components
SR-11	Component Authenticity
SR-12	Component Disposal

The BPA Holder's Plan must describe in sufficient detail, beyond high level overview representations, how they will reduce and mitigate SCRM risk through application/mapping of their defined program appropriate security controls outlined and described in the most current versions of CNSSI 1253, Appendix D, NIST SP 800-53, NIST SP 800-161, and related industry standards **as of the closing date of the RFQ**. Any Information Security Management Systems (e.g., ISO 27K series) controls, or related program standards, should be mapped to their associated NIST baseline controls, where applicable.

The supply chain as reflected in the SCRM plan must span from the lowest sub-component producer or manufacturer to the delivery point of the BPA Holder, or its designated agent, through third party installation, maintenance, and support. The SCRM plan, implementation, and risk assessment methodology processes must follow Appendix D and E of NIST SP 800-161 and NISTIR 7622 guidelines, ensuring application to the BPA Holder and their suppliers, partners, distributors, and any other entity that is responsible for handling or managing the supply chain of the products and services offered under these BPAs. All SCRM plan requirements must also flow down to subcontractor(s). The Prime must be responsible for SCRM plan implementation and adhere to reporting requirements represented by the defined relationship.

If the BPA Holder uses dealers/resellers in the performance of work under the BPA, the SCRM plan must address the use of participating dealers/resellers and provide a listing of each participating dealer/reseller who is permitted to fulfill orders under the BPA.

NOTE: **Within 12 months after BPA award** all identified participating dealers/resellers specified in the SCRM plan must be International Organization for Standardization (ISO) 9001:2015 certified and maintain certification for the remaining performance period of the BPA. Should any participating dealers/resellers not obtain ISO 9001:2015 certification within 12 months after BPA award, the participating dealer/reseller will not be permitted to fulfill orders.

7.4.2.2 Vendor Risk Assessment Program - C-SCRM Monitoring

Upon award, GSA will execute their Vendor Risk Assessment Program (VRAP) as an on-going enterprise approach to continuously manage risk and vulnerabilities associated with the acquisition and sustainment of products or services provided by the BPA Holder. VRAP is a post-award execution activity from an oversight perspective. The program leverages big data analytics to identify, categorize, and assess risk information based on the Risk Factors listed in Table 2. GSA's VRAP utilizes customer defined priorities and risk tolerances, along with twelve defined Risk Factors, to compartmentalize risk findings and provide a well-defined process. As part of the VRAP, GSA may utilize supplier illumination tools to monitor and evaluate risks to its customer's supply chains. GSA reserves the right to identify to the BPA Holder for evaluation, known or potential risks in delivery order execution related to suppliers of products and ancillary services. The BPA Holder must provide any information requested by the Government to facilitate a Vendor Risk Assessment (VRA) **within 10 business days of receiving a written request.**

TABLE 2: Risk Factors and Definitions

Analytical Categories	Risk Factor	Description
Technical	**Quality Assurance**	Customer reviews, adherence to quality standards.
	Production / Manufacturing	Production/manufacturing strategy, plans, and implementation. Current state relative to controls and practices for assuring authenticity and integrity of product/service as received by the end-user, and instances of reported or alleged counterfeit product or fraudulent practices.
	R&D / Innovation	Current state, investment in and plans for product/process improvements and advancements.
Business Management	**Leadership & Organization**	Current and prior affiliations and associations of company leaders. Current state, strategy and plans relative to the organization of the operating unit and relationship to parent, subsidiary or affiliated organizations.
	Supplier Management	Current state, strategy and plans relative to suppliers and supply chain management.
	Business Alliances	Current state, strategy and plans relative to key joint ventures, partnerships, acquisitions, and agreements (including technology/intellectual property).
Market	**Revenue/Financial Health**	Financial status, sources of investment, and revenues by category/source, including indirect and direct funding from U.S. Government organizations.
	Industry/Market Position	Current state, strategy and plans relative to the market/industrial environment, potential customers, and competitors.
	Regulatory & Legal	Status relative to regulatory/legal trends, actions, issues and concerns.
Security	**Socioeconomic Environment**	Current state, trends, issues and concerns relative to the geographical locations and socioeconomic conditions in which the business/enterprise is operating.
	Cybersecurity	Current state, issues, and concerns relative to cybersecurity. Technical vulnerabilities, instances of cyber breach or historic trends.

	Physical Security & Insider Threat	Physical security employed at design, manufacturing, packaging and distribution facilities. Security issues and concerns emanating from people involved with the operating unit, including employees, former employees, Contractors and business associates.

7.4.2.3 Ongoing C-SCRM Monitoring

During the BPA period of performance, the BPA Holder must provide an annual report to the Contracting Officer, Program Manager, and COR on their SCRM activities related to the BPA **due annually upon the anniversary date of the BPA award**. The report must include reporting on the detection of all SCRM compromises/incidences associated with the performance under the BPA, mitigation actions taken, and any resultant impacts to hardware, software, firmware, and data/information consistent with NIST SP 800-161, Appendix D – Incident Response Control Requirements. GSA reserves the right to verify performance against SCRM plan requirements through assessment and inspection of the BPA Holder's facilities and programs in accordance with proper notification procedures and contractual clauses. Successful incident identification and remediation will be viewed favorably with respect to overall strength of SCRM security program execution.

The BPA Holder must also provide a SCRM Plan update to the Contracting Officer, Program Manager, and the COR within 10 business days whenever there is a substantial change that affects one or more CNSSI 1253 security controls. At a minimum the following events substantiate the need for an update: changes in company ownership, changes in senior company leadership, supplier changes, including new capabilities added through new vendors or components, subcontractor changes, and Information and Communication Technology (ICT) supply chain compromises.

7.4.2.4 Off-Ramping - SCRM + VRAP Elements

GSA reserves the unilateral right to Off-Ramp nonperforming BPA Holders. BPA Holders that are Off-Ramped must still complete active orders at the time of the Off-Ramping. Off-ramping methods may result from one of the following conditions:

A. Failure to meet SCRM and SCRM reporting requirements in sections 7.4.2 or failure to remediate successive, repeated security process control failures (greater than two) within the annual reporting cycle. Additional audit/inspection assessment visits may be executed by the Government team to validate compliance.

B. BPA Holders assessed as high-risk relative to defined VRAP factors in Table 2 of Section 7.4.2.2 and the SCRM Factor Information Disclosure Request. Additional audit/inspection assessment visits may be executed by the Government team to validate responses.

If a BPA Holder does not meet these requirements, the Government may "Off-Ramp" the BPA Holder by cancelling the BPA.

7.5 Customer Service

The BPA Holder must provide 24 hours per day, 7 days per week access to customer service via a toll-free

number with real time assistance for EVSE and data access systems as well as a customer service email address. The BPA Holder must be equipped to address EVSE hardware issues and network/connectivity issues both remotely (via phone or internet) and on site by a qualified technician, as needed.

7.6 Delivery

a) Timeframe after receipt of order (ARO) to CONUS locations must be within:
   - 45 calendar days for Level 1 and Level 2
   - 90 calendar days for DC Fast or any other Charging Types/Non-conventional EVSE offerings.

b) Timeframe after receipt of order (ARO) to OCONUS locations must be within:
   - 60 calendar days for Level 1 and Level 2
   - 105 calendar days for DC Fast or any other Charging Types/Non-conventional EVSE offerings.

c) EVSE must be in operable condition and free of defect. Damaged EVSE may be rejected. If the damage is not readily apparent at the time of delivery, the BPA Holder must permit the EVSE to be returned within a reasonable time at no cost to the Government.

d) When Orders include the EVSE with EVSE site assessment, planning or any other related services, the BPA Holder must provide a detailed plan to support the rapid deployment of the EVSE inclusive of the number of days to completion.

7.7 Reporting Requirement

The BPA Holder must submit quarterly sales reports to the COR. The report coverage must include sales information for the preceding quarter. The report must be submitted regardless of whether sales were made and include the following information:

- BPA number
- Order/call number
- Customer name
- Location shipped to or installed (City and State)
- CLIN(s) ordered
- Quantity of units ordered
- Price per unit paid, and
- Total dollar value of order/call

Reports are due January 15th, April 15th, July 15th and October 15th. Reports will be reviewed by the Government within 30 calendar days and during this period the Government may ask for clarifications or additional information. After 30 calendar days, unless otherwise indicated, the report will be considered acceptable.