

**Joint Enabling Capabilities Command (JECC)**  
**Emergency Power Generation Station Preventative Maintenance (PM) Service for**  
**Caterpillar (CAT) Generator (GEN), Uninterrupted Power Supply (UPS), and Automatic**  
**Transfer Switches (ATS) with Switchgear/Circuit Breakers**

**1.0 Scope:** The proposed acquisition is to acquire quarterly and annual PM service and inspection on emergency power generation system for one generator, one UPS unit, and an ATS with switchgear/circuit breakers. These systems are managed by JECC and are located at building X-132 on the Naval Station (NAVSTA) Norfolk, VA. The specific equipment to be serviced under this contract is as follows:

**1.1 Building X-132 NAVSTA Norfolk VA**

- (a) CAT Engine/Generator, Model Number 3412 (800 Kilowatt (kW) serial number 9EP02081
- (b) ATS, Automatic Switch Company (ASCO) 7000 (Series ATS) serial number 191016
- (c) CAT UPS (300kVA) serial number CPZ00306

**2.0 Background:** The JECC provides mission-tailored, joint capability packages to Combatant Commanders in order to facilitate rapid establishment of Joint Force Headquarters, fulfill Immediate Response Force mission execution, and bridge joint operational requirements for 24 hours a day / seven (7) days a week operations. This equipment shall be kept 100% capable and reliable.

**3.0 Objectives:** The contractor shall provide PM support to each Emergency Power Generation station per the PM level specification descriptions below and in accordance with (IAW) the attached inspection checklists. For the generator, ATS and switchgear equipment, the contractor shall provide Level I, Level II and Level III inspection and PM services per the service and maintenance schedule as described in paragraph 4.1.5.

**4.0 Specific Tasks Required:**

All work, service, and maintenance shall be in accordance with (IAW) the manufacturer's recommendations and specifications, and all parts shall be original equipment manufacturer (OEM) and IAW the below schedule.

**4.1 Quarterly Inspections and PM**

**4.1.1 Perform Quarterly Level I Inspection and PM:** See Attachment 1 – PM Level I Item List

**4.1.2 Perform Quarterly Level II Inspection and PM:** See Attachment 2 – PM Level II List

**4.1.3 Perform Level III Inspection and PM:** See Attachment 3 – PM Level III List and see Attachment 4 – PM Checklist form.

**4.1.4 Perform Annual Inspection/Service of ATS and Switchgear**

**4.1.5 ATS PM:** Perform PM of ATS Normal Circuit and Emergency Switch to Manufacturers specification. Change batteries in Programmable Logic Controller (PLC) and Circuit Breaker Trip Units. See Attachment 5 - ATS Inspection and Cleaning Report.

#### 4.1.6 Equipment PM Schedule:

The contractor shall provide PM support as specified in the table below.

| Base Period     |          | Option Period 1 |           | Option Period 2 |          |
|-----------------|----------|-----------------|-----------|-----------------|----------|
| Quarter (Q)     | PM Level | Quarter         | PM Level  | Quarter         | PM Level |
| Q1              | II       | Q1              | II & III* | Q1              | II       |
| Q2              | I        | Q2              | I         | Q2              | I        |
| Q3              | I        | Q3              | I         | Q3              | I        |
| Q4              | I        | Q4              | I         | Q4              | I        |
| Option Period 3 |          | Option Period 4 |           |                 |          |
| Quarter (Q)     | PM Level | Quarter         | PM Level  |                 |          |
| Q1              | II       | Q1              | II & III* |                 |          |
| Q2              | I        | Q2              | I         |                 |          |
| Q3              | I        | Q3              | I         |                 |          |
| Q4              | I        | Q4              | I         |                 |          |

\* PM Level III Inspection only occurs during Option Periods 1 and 4.

4.1.7 Provide onsite UPS maintenance to One (1) CAT UPS IAW the following requirements:

4.1.7.1 Caterpillar UPS (300kVA) Service Requirements

4.1.7.1.1 Quarterly PM – perform IAW checklist provided. See Attachment 6, Caterpillar UPS Inspection and Cleaning Report.

4.1.8 The contractor shall replace any Government-provided original equipment manufacturer spare parts and materials with equivalent original equipment manufacturer parts for restocking as spares.

#### 4.2 Routine and/or Urgent Repair/Service

##### 4.2.1 Routine and/or Urgent Maintenance – Diagnosis, Repair, and/or Service:

The contract will include a service call/repair labor amount and a materials/parts amount for routine and/or urgent repairs. These routine and/or urgent repairs may include, but are not limited to, the following ten (10) most common routine/urgent repairs required of this contract:

##### GEN (800Kw)

1. Replace jacket water heater, thermostats and hoses
2. Replace Global Power Supply (GPS) Input/output (I/O) circuit board
3. Replace starter, battery charger and batteries
4. Replace day tank motor
5. Replace fan and alternator belts
6. Repair low oil pressure shutdown condition

##### UPS

1. (300 kilo-volt-ampere (kVA)) - repair fan failure
2. (300 kVA) - replace fuses
3. (300 kVA) - repair vacuum pump

## **ATS**

1. Replace micro-logic trip unit

The contractor shall ensure parts availability for the 10 most frequent urgent repairs.

### **4.3 Emergency Repair/Service:**

#### **4.3.1 Emergency Maintenance - Diagnosis and Repair:**

The contract will have a travel/labor budget amount for diagnosing emergency repairs and required repair parts resulting from a sudden failure or potential failure, which presents an operating hazard for the equipment.

**4.3.1.1** The Deputy Director of Logistics, phone 757-278-6852, mobile 757-289-9538, and primary Technical Advisor (TA), phone 757-278-6851, or his designated agent, will notify the contractor in the event of a catastrophic equipment failure. A catastrophic equipment failure exists when there is no commercial or generator power available. This service, for diagnosis only, shall be performed within 4 hours of the initial service call. Response for non-catastrophic equipment failures, such as available commercial power but the generator is inoperative, shall be performed within 24-hours of the service call.

**4.3.1.1.1** The TA, or designated agent, will request a service call from the contractor to open, inspect and/or evaluate the equipment as required to determine the cause of the failure. The contractor shall provide a written proposal to identify the deficiencies, listing all supplies, materials, labor hours required and other charges to restore full operational capabilities of the equipment. The written proposal shall be emailed as an email attachment to the requestor (TA or designated agent) to [JECC-HQ-J4-Facilities@groups.mail.mil](mailto:JECC-HQ-J4-Facilities@groups.mail.mil).

### **4.4 General Information:**

**4.4.1.** Due to the specialized nature of the UPS and ATS systems, contractor service technicians and mechanics performing any service, maintenance and repairs shall be trained and certified to service Caterpillar Power Generation equipment and shall provide proof of certification.

**4.4.2.** All services under this contract are considered “Essential Contractor Services” as defined in DFARS 252.237-7023 “Continuation of Essential Contractor Services”.

**4.4.3.** The contractor shall conduct oil and coolant sample and analysis quarterly; results provided to JECC TA and/or Facility Manager within 7 business days. The results shall be emailed as an email attachment to the TA or designated agent to [JECC-HQ-J4-Facilities@groups.mail.mil](mailto:JECC-HQ-J4-Facilities@groups.mail.mil).

**4.4.4.** The contractor shall test fuel storage tank and tank fuel with a visual/sample and analysis annually; results shall be provided to JECC TA and/or Facility Manager within 7 business days. The results shall be emailed as an email attachment to the TA or designated agent to [JECC-HQ-J4-Facilities@groups.mail.mil](mailto:JECC-HQ-J4-Facilities@groups.mail.mil).

**4.4.5.** The contractor shall have access to and maintain all current technical bulletins, warnings and procedural updates to manuals relevant for this equipment.

## **5.0 Deliverables:**

**5.1** Following each PM inspection, a written report shall be provided that details the results of the inspection and shall include specific recommendations toward future remedial actions, upgrades or spares.

**5.2** Quarterly service and inspection reports and repair recommendations with cost proposals for any deficiencies found.

**5.3** Annual service and inspection reports and repair recommendations with cost proposals for any deficiencies found.

**5.4** The contractor shall prepare and deliver copies of the inspection check lists after each service to the Government Site Facility Manager. Contractor format is acceptable.

**6.0 Security Clearance:** Work on this task does not require a security clearance.

## **7.0 Qualifications**

**7.1** The contractor shall provide documentation showing extensive experience in the installation of new, and service and maintenance of, emergency power generation stations complete with ATS and UPS systems in the Hampton Roads, VA area.

**7.2** The contractor shall provide records of past service and maintenance contracts including type and manufacturer of that equipment installed and serviced.

**7.3** The contractor shall provide certifications of training and representation by the equipment manufacturers mentioned in this SOW.

**8.0 Place of Performance:** Work shall be performed at: Building X-132, 9712 Virginia Avenue (Ave), Norfolk VA, 23511, NAVSTA Norfolk; located on the corner of Dillingham Boulevard (Blvd) and Virginia Ave.

**8.1** The above location is a military installation requiring background checks for all contractor personnel gaining access. The contractor shall have Defense Biometric Identification System (DBIDS) for any personnel entering the NAVY base. This is a requirement for award of the contract.

## **9.0 Period of Performance:**

Base Period: 1 January 2027 – 31 December 2027

Option Period 1: 1 January 2028 – 31 December 2028

Option Period 2: 1 January 2029 – 31 December 2029

Option Period 3: 1 January 2030 – 31 December 2030

Option Period 4: 1 January 2031 – 31 December 2031

**10.0 Building X-132, NAVSTA Norfolk Virginia, Site Facility Manager** (these assigned agents are for access coordination to building and equipment)

Name: Mr. Michael Frederick, Facility Manager, (757-278-6851);

Email: [michael.j.frederick6.civ@mail.mil](mailto:michael.j.frederick6.civ@mail.mil)

Name: Mr. Freddie Atkins, Deputy Director, (757-278-6852);

Email: [freddie.w.atkins.civ@mail.mil](mailto:freddie.w.atkins.civ@mail.mil)

## **11.0 CYBERSECURITY**

### **11.1. Operationally Critical Support**

The services designated under this contract are “operationally critical support” as defined in DFARS 252.204-7012.

### **11.2. Cybersecurity Incident Reporting**

**11.2.1.** In addition to the DFARS 252.204-7012 reporting requirements for unclassified systems and DoD Manual (DoDM) 5220.22, National Industrial Security Program Operating Manual (NISPOM) for classified systems, reportable cyber-incidents include, but are not limited to, the following:

**11.2.1.1.** Cyber-incidents as defined in Table 1.

**11.2.1.2.** Notifications by a federal, state, or local law enforcement agency or cyber-center (i.e., National Cyber Investigative Joint Task Force (NCIJTF), National Cybersecurity & Communications Integration Center (NCCIC)) of being a victim of a successful or unsuccessful cyber-event, anomaly, incident, insider threat, breach, intrusion, or exfiltration.

Table 1.

| <b>Incident Category</b> | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root Level Intrusion     | Unauthorized privileged access to an IS. Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category. |
| User Level Intrusion     | Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code   |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | that provides remote interactive control, it will be reported in this category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Denial of Service | Denial of Service (Incident)—Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Malicious Logic   | Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Root or User Level Intrusion incidents. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS. |
| Ransomware        | Malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. Ransomware is a reportable incident that may be associated with multiple incident categories depending on the attack vector and execution.                                                                                                   |

**11.2.2.** If the cyber-incident affects a classified system, vulnerabilities associated with the incident will be classified per the current version of USTRANSCOM Instruction 31-02, Security Classification Guide.

### **11.3. Cybersecurity Incident Reporting Timelines**

In addition to providing the notification required by DFARS 252.204-7012, the contractor is required to notify USTRANSCOM as soon as practical, but no later than 72 hours after discovering a reportable cyber-incident. The reporting timeline begins when the incident is discovered or reported to the company, its employees, contractors, or cybersecurity firm responsible for providing cybersecurity and response for the company. The contractor shall contact the USTRANSCOM Cyber Operations Center (CyOC) via phone at 618-817-4222. If the contractor does not immediately reach the CyOC via phone, the contractor shall send an email notification to [transcom.scott.tcj6.mbx.cyoc-dodin-operations@mail.mil](mailto:transcom.scott.tcj6.mbx.cyoc-dodin-operations@mail.mil).

### **11.4. Mandatory Reporting Data**

**11.4.1.** The contractor shall work with the USTRANSCOM CyOC through resolution of the incident. Within 72 hours of becoming aware of a reportable cyber-incident, the contractor shall provide an initial notification of the incident, even if some details are not yet available, which includes, but is not limited to, the following information:

- (a) Company Name
- (b) Who will be the POC with contact information
- (c) Contracting Officer POC (name, telephone, email)

- (d) Overall Assessment –Description of incident, data at risk, mitigations applied
- (e) Indicators of compromise
- (f) Vector of attack (if known)
- (g) Estimated time of attack (if known)

**11.4.2.** The contractor shall provide a follow-on cyber-incident report to the USTRANSCOM CyOC within 5 days of becoming aware of a reportable cyber-incident, which includes, but is not limited to, the following information:

- (a) Contractor unique Commercial and Government Entity (CAGE) code
- (b) Contract numbers affected
- (c) Facility CAGE code where the incident occurred if different than the prime contractor location
- (d) POC if different than the POC recorded in the System for Award Management (name, address, position, telephone, email)
- (e) Contracting Officer POC (name, telephone, email)
- (f) Contract clearance level
- (g) DoD programs, platforms, systems, or information involved
- (h) Location(s) of compromise
- (i) Date incident discovered
- (j) Type of compromise (e.g., unauthorized access, inadvertent release, other)
- (k) Description of technical information compromised
- (l) Any additional information relevant to the information compromise

## **11.5. Incident Reporting Coordination**

**11.5.1.** In the event of a cyber-incident, USTRANSCOM may conduct an on-site review of network or information systems where DoD information is resident on or transiting to assist the contractor in evaluating the extent of the incident and to share information in an effort to minimize the impact to both parties. Date and time of on-site visits will be mutually agreed upon by USTRANSCOM and the contractor in advance.

**11.5.2.** The contractor agrees to allow follow-on actions by the Government (e.g., USTRANSCOM, Federal Bureau of Investigation, Department of Homeland Security, DC3, etc.) to further characterize and evaluate the suspect activity. The contractor acknowledges that damage assessments might be necessary to ascertain an incident methodology and identify systems compromised as a result of the incident. Once an incident is identified, the contractor agrees to take all reasonable and appropriate steps to preserve any and all evidence, information, data, logs, electronic files and similar type information (reference NIST Special Publication 800-61, Computer Security Incident Handling Guide, (current version)) related to the incident for subsequent forensic analysis so that an accurate and complete damage assessment can be accomplished by the Government.

**11.5.3.** The contractor is not required to maintain an organic forensic capability, but must ensure data is preserved (e.g., remove an affected system, while still powered on, from the network) and all actions documented until forensic analysis can be performed by the Government or, if the

Government is unable to conduct the forensic analysis, a mutually agreed upon third party (e.g., Federally Funded Research and Development Center (FFRDC), commercial security contractor, etc.). Any follow-on actions shall be coordinated with the contractor via the Contracting Officer.

**11.5.4.** The contractor agrees to indemnify and hold the government harmless for following any recommendations to remedy or mitigate the cyber-incident following the actions under 11.5.1. and 11.5.2.

#### **11.6. Confidentiality and Non-Attribution Statement**

The Government may use and disclose reported information as authorized by law and will only provide attribution information on a need-to-know basis to authorized persons for cybersecurity and related purposes (e.g., in support of forensic analysis, incident response, compromise or damage assessments, law enforcement, counterintelligence, threat reporting, and trend analysis). The Government may share threat information with other USTRANSCOM industry partners without attributing or identifying the affected contractor.

**Attachment 1**  
**LEVEL I INSPECTION & MAINTENANCE SERVICE**  
**SCOPE OF WORK**

**LEVEL I INSPECTION:**

99 Point Generator Inspection includes:

1. Engine
2. Lubrication System
3. Cooling System
4. Fuel System
5. Air Induction and Exhaust System
6. Electrical Systems
7. Fluid Sampling and Analysis (results normally within 48 hours)
8. Inspection report and repair recommendations
9. Inspect generator main circuit breaker

**Attachment 2**  
**LEVEL II INSPECTION & MAINTENANCE SERVICE**  
**SCOPE OF WORK**

**LEVEL II INSPECTION:**

99 Point Generator Inspection includes:

1. Engine
2. Lubrication System
3. Cooling System
4. Fuel System
5. Air Induction and Exhaust System
6. Electrical Systems
7. Fluid Sampling and Analysis (results normally within 48 hours)
8. Inspection Report and repair Recommendations
9. Change Engine Oil (Materials Included)
10. Replace Engine Oil and Fuel Filters (Materials Included)
11. Dispose of All Waste Oil and Materials
12. Inspect turbocharger (if equipped)
13. Inspect Generator Bearings (as required)
14. Insulation Resistance Test

**Attachment 3**  
**LEVEL III INSPECTION & MAINTENANCE SERVICE**  
**SCOPE OF WORK**

**LEVEL III INSPECTION & MAINTENANCE**

**Space Heaters**

1. Check for proper operations (if equipped)

**Generator**

2. Check for moisture, dust, oils, greases, and debris on main stator windings, exciter, and Permanent Magnet Generator (PMG) (clean as needed)
3. 4-hour load bank test at 100% resistive load

**Cooling System**

1. Drain, and fill engine coolant
2. Replace thermostat(s)

**Hoses and Belts**

1. Replace coolant hoses
2. Replace drive belts

**Batteries**

1. Replace engine starting batteries

**Turbocharger**

2. Inspect for proper operation
3. Check the end play and radial clearance on turbine wheel and shaft

**Engine**

1. Adjust engine valves

**Generator Bearing**

2. Inspect bearing and bracket



Attachment 4 - PM  
INSPECTION SHEET.p



Attachment 5 - ATS  
INSPECTION SHEET.p



Attachment 6 - UPS  
INSPECTION FORM.p

DRAFT