

Department of Veterans Affairs
STATEMENT OF WORK (SOW)
Multi-Function Device Lease & Maintenance Service

1. General Information

1.1 Description of services: The Department of Veterans Affairs, Veterans Benefits Administration, Detroit Regional Office has a requirement for a 60 month Lease with a Flat-Rate Monthly Fee Copying plan for 17 new copy Machines which includes all consumable supplies (except copying paper), and full maintenance services including repair parts. **The VA intends to make a single (all or none), firm-fixed-price award for a 12 month period with four (4) option years.**

1.2 Background: The Department of Veterans Affairs, Detroit VA Regional Office, has a requirement to acquire copiers for the duplication of the various documents it uses to perform its mission. The primary role of the machines to be leased will be for functioned copying. The Government would like to accomplish these tasks through the use of 17 leased copiers. The contract can be modified to add additional lease copiers, with prior written notification from the Contracting Officer.

1.3 Scope of work: The contractor shall furnish all repair parts, labor, transportation, and supplies required to accomplish inspecting, cleaning, lubricating, adjusting, calibrating, and vacuuming (if required), and repairing of the copiers. Contractor shall maintain the leased copiers at levels necessary to provide the specified functions to meet the manufacturer's current equipment specifications. The 60 month lease includes a Flat-Rate Monthly Fee Copying Plan with NO intent to purchase the equipment at the end of the lease agreement period. Ownership of the asset/copiers remains with the prospective contractor.

1.4 Period of Performance: **The base year Period of Performance will be 12 months from award date with four (4) twelve (12) month option years.**

1.5 Safety Requirements: While in performance of the resultant contract, the contractor shall maintain safety and health standards compliant with requirements of the Occupational Safety and Health Administration (OSHA) and adhere to VAAR 852.237-70 Contractor responsibilities.

1.6 Security Requirements: Contractor personnel will be required to contact the government designated point of contact upon arrival when reporting for service calls or delivering supplies. The contractor shall be responsible for the security of all organizational information. Current rules and regulations applicable to the premises, where the work shall be performed, shall apply to the contractor and its employees while working on the premises. These regulations include but are not limited to, escort by VBA officials, presenting valid identification, smoking restriction and any safety procedures as outlined in the site regulations. Services will not require connection to the VA network. The C&A requirements do not apply and a Security Accreditation Package is not required.

1.6.1 The contractor shall not disclose or cause to disseminate any information concerning operations of Department of Veterans Affairs. Such action(s) could result in violation of the contract and possible legal actions.

1.6.2 All inquiries, comments, or complaints arising from any matter observed, experienced, or learned of as a result of or in connection with the performance of the contract, the resolution of which may require the dissemination of official information, shall be directed to the government's designated representative.

1.7 No overage charges: The government pays a flat-rate monthly fee per copier, regardless of the number of copies made each month. The copy volume allowance per month is unlimited per copier.

1.8 Termination Amortization Schedule: A termination amortization schedule shall be included as an attachment of the awarded contract. **If the Government does not exercise any of the options listed in the Price/ Cost Schedule, the Government's not exercising the options will have the same effect as if the Government terminated for convenience. All remedies afforded to contractor in regards to a termination for convenience shall be available to the contractor.**

1.9 Invoices: Contractor shall email invoices monthly in arrears to the email address listed on page one (1) block 18a that include the following information: 1) Contract and obligation numbers; 2) Company name, address and phone number; 3) Monthly contracted lease rate (which includes the maintenance service fee); 4) Invoice number and date (note that each invoice must have a different invoice number).

Part 2. Definition and Acronyms: N/A

Part 3. Government-Furnished Items and Services. The Government shall supply the paper for the copiers.

Part 4. Contractor-Furnished Items and Services

4.1 Required personnel, materials, supplies, and equipment: The contractor shall furnish all personnel, materials, supplies, and equipment required to perform work under the contract, to include but not limited to tools and expendable items. The Flat-Rate Monthly Fee Copying Plan must include new equipment, full service maintenance, preventative maintenance, repair parts, all operational/consumable supplies such as toner, dry ink, fuser oil, staples and other copier supplies for the copier, except paper. The following table includes the install locations, copies per minute, quantity, estimated monthly volume and output type of the copiers which the contractor shall delivered/setup and install.

QUANTITY	COPIES PER MINUTE	OUTPUT TYPE	ESTIMATED COPIES PER MONTH PER COPIER
477 Michigan Avenue Room 1445 Detroit, MI 48226			
12	42	B/W	10,000
1	52	B/W	20,000
1	62	B/W	45,000
3001 Coolidge Rd. Suite 401 East Lansing, MI 48823			
1	30	B/W	2,500
110 Michigan St. NW Room 436 Grand Rapids, MI 49503			
1	35	B/W	5,000
200 N. Main Street Room 310 Mt. Pleasant, MI 48858			
1	35	B/W	5,000

4.1.1 The copiers shall have the following minimum requirements:

4.1.1.1 **30 ppm:** B&W MF Copiers with Reversing Automatic Document Feeder, 1000 Sheet, Finisher/Stapler , Data Security Kit, Stand, Standard Network Print/Scan

4.1.1.2 **35 ppm** B&W MF Copiers with -Dual Scan Automatic Document Feeder, 3000 Sheet Large Capacity Paper Tray (Copier comes standard with 2 x 500 sheet trays in addition), Fax

4.1.1.3 **42 ppm:** B&W MF Copiers with Dual Side Scanning Document Feeder (Scans both sides of the page in a single pass), 1000 Sheet Finisher/Stapler, Data Security Kit (Hard Drive Erase), 2 standard 500 sheet paper trays up to 11 x 17, Copier Stand , Standard Network Print/Scan.

4.1.1.4 **52 ppm:** B&W MF Copiers with Dual Side Scanning Document Feeder (Scans both sides of the page in a single pass), 1000 Sheet Finisher/Stapler, Data Security Kit (Hard Drive Erase), 2 standard 500 sheet paper trays up to 11 x 17, Copier Stand , Standard Network Print/Scan.

4.1.1.5 **62 ppm:** B&W MF Copiers with Document Feeder, 3000 Sheet Finisher/Stapling, Hole Punch, 4000 Sheet High Capacity Paper Drawer, Data Security Kit, Network Print/Scan.

4.1.1.6 Energy Star compliant.

4.1.1.7 Power source: 110 volt 15 amp

4.1.1.8 EPEAT-Registered Bronze level or higher.

4.2 Delivery: The contractor will coordinate the delivery, installation and training date with the designated government employee. The government will provide the contractor with dock access and

building access for this sole purpose. The government requires a minimum of 24 hour notice of the contractor's need to deliver a copier(s) and/or remove a copier(s) or deliver copier replacement parts. The designated government employee will work with the pertinent government agency (ies) to secure the needed dock access. The delivery truck can be no larger than 45 feet. No deliveries can be made after 4:30 p.m. Driver needs a valid ID.

4.3 Contractor Point of Contact: The contractor shall furnish one designated point of contact (POC) to the government's designated representative for coordination of supplies, delivery, and/or maintenance. The POC will be empowered to make daily decisions to ensure that the contract implementation and day-to-day maintenance meets the terms and conditions of this contract.

4.4 Contractor's Phone Number: The contractor shall provide a toll-free telephone number for service calls, which must be answered during at least eight working hours, between 8:00 am and 4:30 pm, Monday through Friday.

4.5 Parts/Supplies Availability: The contractor shall have an inventory of parts and consumable supplies in quantities sufficient to effectively service the resulting contract. The contractor shall have an internal inventory system and delivery system for the parts and consumable supplies. The inventory and delivery system must be sufficient to service the contract in accordance with the maintenance response times specified in paragraph 5.1 and the supply delivery times specified in paragraphs 5.3., 5.3.1 and 5.3.2.

4.6 Personnel Qualifications: **The contractor shall be required to provide fully qualified and manufacturer trained or certified service, delivery, and management personnel in sufficient numbers to actively and efficiently service and support the copiers in place during the contract period.**

Part 5. Specific Tasks

5.1 Service Calls: The contractor shall respond to service calls during normal working hours, Monday through Friday, excluding holidays observed by the Federal Government. The contractor shall respond to verbal service calls and is expected to initiate the repairs within two (2) working hours after notification of malfunction. The response time on a service call starts when the service call is placed to the contractor. The service technician shall report to the service requestor and notify of his/her arrival and verify the problem for which the service call was made. If the service call is not completed, the service technician shall contact the government's designated representative and provide a detailed explanation as to why the copier was not repaired and provide an estimated time for completion of the required repairs. The contractor shall complete the repairs and satisfactorily resolve the problem by effectively restoring the copier to normal operating capability within eight (8) working hours of responding.

5.1.1 The Contractor shall have an adequate working inventory of copiers in order to provide backup support for the leased 17 copiers. When a malfunctioning copier cannot be repaired within the on-site repair time, the VA will have the option of requesting a backup copier at no additional cost to the government. The Contractor shall supply such a backup copier within seven (7) working hours after notification by the government. Backup copiers shall meet or exceed the capabilities of the copiers to be replaced. For this purpose only, remanufactured equipment may be used as a temporary device

until a new replacement copier is delivered or the original copier is reinstalled. Backup copiers are generally expected to remain in place for five working days or less, but in unusual cases, a backup copier may remain in place for as long as 60 days. If the original copier has not been repaired and reinstalled at the end of 60 days, the Contractor shall provide a replacement copier equal to or superior to the original copier model at no additional cost to the government. The Contractor shall coordinate the removal, delivery and install of the back-up copier with the designated government employee.

5.2 Preventive Maintenance: The contractor shall provide, at a minimum, one annual preventive maintenance service call to ensure that the copiers are maintained in fully operational condition. Contractor shall maintain the copiers in at levels necessary to provide the specified functions to meet the manufacturer's current equipment specifications.

5.3 Replenishment of Supplies Procedures: On or about the same day of each month, the contractor shall ensure that each copier is furnished with sufficient consumable supplies, (excluding paper) to produce a volume of copies equal to the levels necessary to provide the specified functions to meet the manufacturer's current equipment specifications. Upon initial delivery of the copy machines/devices, the Contractor shall provide two months' worth of consumable supplies for each copier. These supplies will be stored by the Support Services Division of VARO Cleveland.

5.3.1 The contractor shall respond to verbal requests for additional consumable supplies under the following conditions: The government's designated representative may make emergency requests for consumable supplies verbally. Orders will state the quantity and type of consumable supplies required and the location and serial number of the copier for which the additional consumable supplies are being ordered. The contractor shall deliver additional consumable supplies within a period of twenty-four hours after receipt of verbal order.

5.3.2 Supplies from the contractor shall be delivered between 8:00 a.m. and 4:30 p.m., Monday through Friday (excluding Federal holidays) directly to the copier location.

5.4 Hard-drives: The contractor shall remove the hard-drives from the 17 leased copiers at the end of the term of the contract and hand them to a designated government representative for destruction. Once a device is delivered and installed, the government will retain ownership of the hard drive.

5.5 Training: Contractor shall provide training on the operation of the leased (17) copiers to designated government representatives **within two days of installation date**. The Contractor shall demonstrate that the copier is properly functioning upon completion of installation. This demonstration shall be accomplished pursuant to the operating instructions furnished with each copier and in the presence of designated government representative.

5.6 Relocate Equipment: Should the government elect to relocate its office to another facility/building or location within the greater Detroit area, all copier machines will then be moved to the new location by the government. The government will have the responsibility of transporting all copier machines to the new office location and will ensure that all copy machines are transported with care. The expense of moving/relocating the copier machines will be paid by government.

Part 6. Government Point of Contact: TBA

Part 7. VA Information Custodial Language

7.1. All Contractors and Contractor personnel shall be subject to the same Federal security and privacy laws, regulations, standards and VA policies as VA, including the Privacy Act, 5 U.S.C. §552a, and VA personnel, regarding information and information system security. Contractors must follow policies and procedures outlined in VA Directive 6500, Information Security Program which is available at: <http://www1.va.gov/vapubs> and its handbooks to ensure appropriate security controls are in place.

7.2. The Contractor will not have access to VA Information Systems.

7.3. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor or subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor or subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

7.4. VA information should not be co-mingled, if possible, with any other data on the contractors or subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct onsite inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

7.5. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

7.6. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or

Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

7.7. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

7.8. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for cause or terminate for convenience.

Part 8. Security Incident Investigation

8.1. The term “security incident” means an event that has, or could have, resulted in loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor shall immediately (within 1 hour) notify the CO and simultaneously, the VA Network Security Operations Center (vansoc@va.gov) and the designated ISO/Privacy Officer for the contract of any known or suspected security/privacy incident, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor has access.

8.2. To the extent known by the contractor, the contractor’s notice to VA will identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information/assets were placed at risk or compromised), and any other information that the contractor considers relevant.

8.3. Contractor will simultaneously report the incident to the appropriate law enforcement entity(ies) of jurisdiction in instances of theft or break-in. The contractor, its employees, and its subcontractors and their employees will cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor will cooperate with VA in any civil litigation to recover VA information, to obtain monetary or other compensation from a third party for damages arising from any incident, or to obtain injunctive relief against any third party arising from, or related to, the incident.

8.4. To the extent practicable, contractor shall mitigate any harmful effects on individuals whose VA information was accessed or disclosed in a security incident. In the event of a data breach with respect to any sensitive personal information processed or maintained by the contractor or subcontractor under the contract, the contractor is responsible for liquidated damages of \$37.50 per affected individual to be paid to VA.

8.5 Liquidated Damages for Data Breach: Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for

liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the contractor provides payment of actual damages in an amount determined to be adequate by the agency.

Part 9. Contractor Rules and Behavior

Contractor agrees to abide by these terms and account for the “I” and “my” and “me” used in these rules.

This User Agreement contains rights and authorizations regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the Department of Veterans Affairs (VA). This User Agreement covers my access to all VA data whether electronic or hard copy ("Data"), VA information systems and resources ("Systems"), and VA sites ("Sites"). This User Agreement incorporates Rules of Behavior for using VA, and other information systems and resources under the contract.

9.1. GENERAL TERMS AND CONDITIONS FOR ALL ACTIONS AND ACTIVITIES UNDER THE CONTRACT:

9.1.1 I understand and agree that I have no reasonable expectation of privacy in accessing or using any VA, or other Federal Government information systems.

9.1.2 I consent to reviews and actions by the Office of Information & Technology (OI&T) staff designated and authorized by the VA Chief Information Officer (CIO) and to the VA OIG regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA. These actions may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing to all authorized OI&T, VA, and law enforcement personnel as directed by the VA CIO without my prior consent or notification.

9.1.3 I consent to reviews and actions by authorized VA systems administrators and Information Security Officers solely for protection of the VA infrastructure, including, but not limited to monitoring, recording, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized OI&T, VA, and law enforcement personnel.

9.1.4 I understand and accept that unauthorized attempts or acts to access, upload, change, or delete information on Federal Government systems; modify Federal government systems; deny access to Federal government systems; accrue resources for unauthorized use on Federal government systems; or otherwise misuse Federal government systems or resources are prohibited.

9.1.5 I understand that such unauthorized attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. This includes penalties for violations of Federal laws including, but not limited to, 18 U.S.C. §1030 (fraud and related activity in connection with computers) and 18 U.S.C. §2701 (unlawful access to stored communications).

9.1.6 I agree that OI&T staff, in the course of obtaining access to information or systems on my behalf for performance under the contract, may provide information about me including, but not limited to, appropriate unique personal identifiers such as date of birth and social security number to other system administrators, Information Security Officers (ISOs), or other authorized staff without further notifying me or obtaining additional written or verbal permission from me.

9.1.7 I understand I must comply with VA's security and data privacy directives and handbooks. I understand that copies of those directives and handbooks can be obtained from the Contracting Officer. If the contractor believes the policies and guidance provided by the Contracting Officer is a material unilateral change to the contract, the contractor must elevate such concerns to the Contracting Officer for resolution.

9.1.8 I will report suspected or identified information security/privacy incidents to the Contracting Officer and to the local ISO or Privacy Officer as appropriate.

9.2. GENERAL RULES OF BEHAVIOR

9.2.1 Rules of Behavior are part of a comprehensive program to provide complete information security. These rules establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the information it contains is an essential part of their job. The following rules apply to all VA contractors. I agree to:

9.2.1.1 Follow established procedures for requesting, accessing, and closing user accounts and access. I will not request or obtain access beyond what is normally granted to users or by what is outlined in the contract.

9.2.1.2 Use only systems, software, databases, and data which I am authorized to use, including any copyright restrictions.

9.2.1.3 I will not use other equipment (OE) (non-contractor owned) for the storage, transfer, or processing of VA sensitive information without a VA CIO approved waiver, unless it has been reviewed and approved by local management and is included in the language of the contract. If authorized to use OE IT equipment, I must ensure that the system meets all applicable 6500 Handbook requirements for OE.

9.2.1.4 Not use my position of trust and access rights to exploit system controls or access information for any reason other than in the performance of the contract.

9.2.1.5 Not attempt to override or disable security, technical, or management controls unless expressly permitted to do so as an explicit requirement under the contract or at the direction of the Contracting Officer or ISO. If I am allowed or required to have a local administrator account on a government-owned computer, that local administrative account does not confer me unrestricted access or use, nor the authority to bypass security or other controls except as expressly permitted by the VA CIO or CIO's designee.

9.2.1.6 Contractors' use of systems, information, or sites is strictly limited to fulfill the terms of the contract. I understand no personal use is authorized. I will only use other Federal government information systems as expressly authorized by the terms of those systems. I accept that the restrictions under ethics regulations and criminal law still apply.

9.2.1.7 Grant access to systems and information only to those who have an official need to know.

9.2.1.8 Protect passwords from access by other individuals.

9.2.1.9 Create and change passwords in accordance with VA Handbook 6500 on systems and any devices protecting VA information as well as the rules of behavior and security settings for the particular system in question.

9.2.1.10 Protect information and systems from unauthorized disclosure, use, modification, or destruction. I will only use encryption that is FIPS 140-2 validated to safeguard VA sensitive information, both safeguarding VA sensitive information in storage and in transit regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA.

9.2.1.11 Follow VA Handbook 6500.1, Electronic Media Sanitization to protect VA information. I will contact the Contracting Officer for policies and guidance on complying with this requirement and will follow the Contracting Officer's orders.

9.2.1.12 Ensure that the Contracting Officer has previously approved VA information for public dissemination, including e-mail communications outside of the VA as appropriate. I will not make any unauthorized disclosure of any VA sensitive information through the use of any means of communication including but not limited to e-mail, instant messaging, online chat, and web bulletin boards or logs.

9.2.1.13 Not host, set up, administer, or run an Internet server related to my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA unless explicitly authorized under the contract or in writing by the Contracting Officer.

9.2.1.14 Protect government property from theft, destruction, or misuse. I will follow VA directives and handbooks on handling Federal government IT equipment, information, and systems. I will not take VA sensitive information from the workplace without authorization from the Contracting Officer.

9.2.1.15 Only use anti-virus software, antispyware, and firewall/intrusion detection software authorized by VA. I will contact the Contracting Officer for policies and guidance on complying with this requirement and will follow the Contracting Officer's orders regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with VA.

9.2.1.16 Not disable or degrade the standard anti-virus software, antispyware, and/or firewall/intrusion detection software on the computer I use to access and use information assets or resources associated

with my performance of services under the contract terms with VA. I will report anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages to the Contracting Officer.

9.2.1.17 Understand that restoration of service of any VA system is a concern of all users of the system.

9.2.1.18 Complete required information security and privacy training, and complete required training for the particular systems to which I require access.

9.3. ADDITIONAL CONDITIONS FOR USE OF NON- VA INFORMATION TECHNOLOGY RESOURCES

9.3.1 When required to complete work under the contract, I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA approved remote access software and services.

9.3.2 Remote access to non-public VA information technology resources is prohibited from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.

9.3.3 I will not have both a VA network line and any kind of non-VA network line including a wireless network card, modem with phone line, or other network device physically connected to my computer at the same time, unless the dual connection is explicitly authorized by the Contracting Officer.

9.3.4 I understand that I may not obviate or evade my responsibility to adhere to VA security requirements by subcontracting any work under any given contract or agreement with VA, and that any subcontractor(s) I engage shall likewise be bound by the same security requirements and penalties for violating the same.

9.4. STATEMENT ON LITIGATION

This User Agreement does not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

9.5. ACKNOWLEDGEMENT AND ACCEPTANCE

I acknowledge receipt of this User Agreement. I understand and accept all terms and conditions of this User Agreement, and I will comply with the terms and conditions of this agreement and any additional VA warning banners, directives, handbooks, notices, or directions regarding access to or use of information systems or information. The terms and conditions of this document do not supersede the terms and conditions of the signatory's employer and VA.

Print or type your full name

Signature

Contractor's Company Name

Position Title

Office Phone

Part 10. Changes to the Statement of Work (SOW):

Any changes to this SOW shall be authorized and approved only through written correspondence from the Contracting Officer. Costs incurred by the contractor through the actions of parties other than the Contracting Officer shall be borne by the contractor.