STATEMENT OF WORK
SHREDDING SERVICES

1. GENERAL SCOPE OF WORK

1.1. The statement of work (SOW) and accompanying Business Associate Agreement (BAA) detail the requirements for the Veteran's Administration Pacific Islands Health Care System (VAPIHCS) for shredding services. Contractor shall provide all labor, supervision, management support, transportation, supplies, equipment and materials necessary to perform shredding services in accordance with privacy, security, and performance requirements as detailed in this SOW. A total of 100 shred bins are required. The following locations shall be serviced with the number of pick up bins in brackets [ ]: At the discretion of the Contracting Officer, this contract may be for one (1) Base year and may include one to four (1-4) Option years.

1.2. **Locations**

1.2.1. Spark M. Matsunaga Medical Center, 459 Patterson Rd, Honolulu, HI 96819, E-Wing and Ambulatory Care Clinic (ACC) [65 containers], Ward 3B2 [1 container], Ward 5C1 [1 container], and the Community Living Center (CLC) [6 containers] [52 pickups per year]

1.2.2. Call Center, Contracting Office, Telehealth, and Home Based Primary Care (HBPC) and VA Warehouse at the Airport Industrial Park, 3375 Koapaka Street, Honolulu, HI 96819 [9 containers] [52 pickups per year]

1.2.3. Maui VA Community Based Outpatient Clinic (CBOC), 203 Ho'ohana Street, Suite 303, Kahului, Hawaii 96732 [3 containers] [26 pickups per year]

1.2.4. Kauai VA Community Based Outpatient Clinic (CBOC), Suite 150, 4485 Pahe'e St., Lihue, HI 96766 [2 containers] [26 pickups per year]

1.2.5. Hilo VA Community Based Outpatient Clinic (CBOC), 1285 Waianuenue Avenue, Suite 211, Hilo, Hawaii 96720 [4 containers] [26 pickups per year]

1.2.6. Kona VA Community Based Outpatient Clinic (CBOC), 75-377 Hualalai Road, Kailua-Kona, Hawaii 96740 [2 containers] [26 pickups per year]

1.2.7. Leeward Oahu VA Community Based Outpatient Clinic (CBOC), 91-2135 Fort Weaver Road Ewa Beach, HI 96706 [2 containers] [52 pickups per year]

1.2.8. Federal Building, 300 Ala Moana Blvd, Honolulu, HI 96850 [4 containers] [52 pickups per year]

1.2.9. Barber's Point 91-1039 Shangrila Road Room 144, Kapolei, HI 96707 [1 container] [12 pickups per year]

2. CONFORMANCE STANDARDS

2.1. Material picked up from the VAPIHCS and its CBOCs shall be destroyed by shredding, wet pulping, macerating, chopping, or otherwise so it's not readable or reconstructable.

2.2. Contractor shall possess current certification, be bonded, and insured as a confidential document destruction company as certified by the National Association for Information Destruction (NAID).

2.3. Contractor shall perform all work in accordance with the guidelines of Federal, State and local ordinances. All safety practices prescribed by these agencies shall be followed.

2.4. Contractor and staff shall comply with the federal Privacy Act of 1974, VA Security regulations, Health Insurance Portability and Accountability Act (HIPAA), and the Archivist of the United States governing methods of destroying records, (36 C.F.R. 1228.58, Destruction of Temporary Records).

2.5. Contractor shall provide a certificate of destruction for each job completed as witness to the interim and final destruction of material collected from the VAPIHCS main campus, it's outlying buildings, and CBOCs. If a contractor (or subcontractor or third party) employee is the witness, then that individual must, prior to departing the VA location, provide the designated VA representative with documentation that acknowledges receipt of the temporary paper records.

2.6. All contractors' staff shall receive privacy training annually.

2.7. Contractor shall be required to sign a Business Associate Agreement (BAA) with VAPIHCS. Please see attachments in Section D of the solicitation/contract.

2.8. Contractor shall be required to sign a Contractor Rules of Behavior and return it to the COR within 30 days of contract award.

2.9. A Contractor Security Control Assessment (CSCA) is required within 30 days of contract approval and annually on the due date of the contract renewal. This should be returned to the Information Security Officer (ISO). The ISO/COR or CO can also request that a CSCA be completed by the contractor anytime there are potential security issues identified or suspected by VA or to ensure that applicable security controls are being implemented.

2.10. The contractor and their personnel shall be subject to the Federal laws, regulations, standards, and VA Directives and Handbooks regarding information and

information system security as delineated in this contract.

3. HOURS OF WORK

3.1. Contractor shall schedule retrieval/pick-up times during normal business hours. Normal business hours for shredding pick-up and bin-exchange services are defined as Monday through Friday from 8:00 am to 4:30 pm, excluding Federal holidays, or as otherwise coordinated with the Contracting Officer Representative (COR) or his/her designee.

3.2. The 10 holidays observed by the Federal Government are: New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day and Christmas Day. Also, any other day declared by the President of the United States to be a national holiday.

4. SUPPLIES

4.1. Contractor shall provide locking shred bins to be placed in designated locations throughout the VAPIHCS and CBOC sites for the collection of paper to be shredded. All locking shred bins shall have a mail slot on top for disposal of paper. Contractor shall provide serial numbered tamper resistant locking ties for all CBOC locations, if shredding is not performed on site.
Contractor shall add additional locking shred bins for new locations with at least one month prior notification at current contract rate.

5. EQUIPMENT

5.1. Contractor shall provide secure shredding services for the VAPIHCS and designated CBOCs. The truck used by the contractor shall be equipped with locking doors to secure shred bags and provide security of information from unauthorized access, weather elements, or loss of data during transport from the VAPIHCS and CBOCs to the final shredding facility site. If interim destruction of materials is provided, these services shall make the material not readable and not reconstructable without extraordinary effort.

5.2. Couriers shall use tamper resistant serial numbered ties on all bags leaving the CBOCs if shredding is not performed onsite. At all times, the secure information and shred bags retrieved from the VAPIHCS sites shall be secure and monitored, from time of pick-up by the contractor, during transport, and during the shredding/baling and final destruction process.

5.3. Material collected for destruction shall be kept in a manner that prevents their content from being read by individuals with no official business need or right to access the data contained in these records. The method of collecting and processing this material shall also prevent the loss or theft of these records until their final destruction.

6. LABOR

6.1. Contractor shall provide labor to collect shred bins/bags from designated facility locations. Access to buildings will be during normal business hours through available VAPIHCS personnel. Contractor shall be responsible for disposing of all shredded material off-site at their own expense. Contractor personnel involved in the actual handling and shredding of documents shall wear a contractor-provided, clearly readable identification badge, which shall display the name of the employee and the company. Contractor personnel's clothes are to be clean and maintained in good repair.

6.2. Contractor shall be required to shred, pulp, macerate, chop, or otherwise definitively destroy the information contained in the bins. The destruction of the information will be witnessed either by a VAPIHCS employee or, as pre-authorized by the VAPIHCS organization, by a contractor employee with subsequent destruction certificates to document the retrieval, transport, shredding, and final destruction of the paper with contractor signature attestation as witness to the shredding.

6.3. Contractor shall provide a key to the lockable shred bin containers to the facility Contracting Officer's Representative (COR) and Privacy Officer to use in case of an emergency. Contractor shall not allow anyone access to the shred containers without permission from the COR, CO, or Privacy Officer. Any damaged or broken locks shall be replaced by the contractor. Shred bin containers shall be labeled and maintained in designated, secure areas of the facility.

6.4. Contractor shall be responsible for collecting shred bins/bags at each facility and secure transport of them to contractor shred site. At no time shall the Contractor leave a collection bin/bag unattended or unlocked. Contractor shall arrive at the designated collection area to begin retrieval of the shred bins/bags and shall perform the necessary transfer/exchange to return the empty containers to those same locations after the retrieval process is complete. A tour of locations of shred bins will be provided by the COR and/or VAPIHCS personnel identified by the COR for other than Honolulu locations.

6.5. Contractor's vehicles used to perform service under this contract shall be locked and the keys removed from the vehicles when not in use. Vehicle(s) shall be identified and parked in a predetermined location agreeable to both the VAPIHCS and the Contractor.

6.6 If an interim destruction of documents is not conducted, Contractor shall provide the facility with documentation that an interim destruction is not practicable.

6.7 Contractor shall provide the facility with documented evidence of the amount and date the material was collected prior to transporting off-site If final data destruction is conducted off-site.

6.8 Contractor shall provide a certification of destruction once the service is complete. Contractor shall provide a written statement of assurance that all documents (sensitive data) intended for shredding were completely destroyed and unreadable utilizing methods

that render the material unreadable and/or unrecoverable. The certificate of destruction shall also state when the documents were destroyed and that all sensitive data is protected from unauthorized disclosure from the point of retrieval from the VAPIHCS and CBOCs to the final destruction facility.

6.9 Included on monthly invoices, Contractor shall provide Contract Line Item Numbers (CLIN). The invoices should mirror the structure of the contract price schedule and itemize the charges as shown in the contract. The invoice should state the description of the service as it appears in the CLIN, date, time, and number of bins serviced. The invoice should include the date of shredding, and poundage of paper shredded for the month being billed.

7. SCHEDULING

7.1. For the solicitation phase, the contractor shall provide information concerning shredding ability and security procedures. This shall include a schedule for pick-up once every week for designated facilities with completion during normal office hours. Additional pickups may be requested as needed for special projects or periods of excessive destruction needs when containers become full before the next scheduled pickup. The contractor shall stipulate what contaminants and other items will not be acceptable in the collection bins. The retrieval-pickup schedule and container placement will be reviewed periodically by contractor and COR together and on an "as-needed" basis to adjust for the maximum usage of the containers.

8. SECURITY REQUIREMENTS

8.1. The performance of this contract requires the Contractor to have routine, unescorted access to the VAPIHCS. VA requires that all Contractor personnel involved in the actual handling and shredding of documents at any facility and who have access to Protected Health Information (PHI) shall undergo FBI National Criminal History Fingerprint Check. All contractor employees shall be the subject of a "low-level security" background investigation (National Agency check with written inquiries; approximate cost $200.00-$300.00) and shall receive a favorable adjudication from the VA Office of Security and Law Enforcement prior to contract performance. This requirement is applicable to all contractor personnel requiring access or responsible for the shredding of VAPIHCS information. The cost for such investigation shall be borne by the contractor. The contractor shall be required to furnish all applicable employee information to conduct the investigation. If the investigation is not completed within 40 days from contract award, the Contractor shall be responsible for the actions of those individuals they provide to perform work for VA. Failure to complete a background investigation may result in contractor personnel being removed from the contract and no longer performing services.

8.2. The Certification and Accreditation (C&A) requirements do not apply, and a Security Accreditation Package is not required.

8.3. Strict adherence to VAs security operations and procedures is required. Contractor shall maintain a current listing of employees. The list shall include the employee's name, address, phone number, social security number, level of security and position. The list shall be validated, maintained, and signed by the Contractor and provided to the Contracting Office on an annual basis. An updated listing shall be provided when an employee's status or information changes. The Contractor has 24 hours to inform the COR that the employee no longer works for them, however if the individual leaves employment on a pick up day, they shall inform the Contracting Office and COR immediately by phone, or e-mail.

8.4. Contractor and Staff shall comply with Homeland Security Presidential Directive-12 (HSPD-12), NIST 800-53, Office of Management and Budget (OMB) guidance M-05-24, as amended, and Federal Information Processing standards Publication (FIPS PUB) Number 201, as amended. These documents are available online.

8.5. Contractor employees are prohibited from possessing weapons, firearms, or ammunition, on themselves or their contractor-owned or privately owned vehicle while on VA property.

8.6. If the Contracting Officer finds it in the best interest of the Government he/she may at any time during the performance of this contract order the Contractor to remove any of his/her personnel from further performance under this contract for reasons of their moral character, unethical conduct, security reasons and violation of on-site building rules. In the event that it becomes necessary to replace any Contractor personnel for any of the above reasons, the Contractor shall bear all costs associated with such removal, including the costs for the replacement of any personnel so removed. These charges shall not be chargeable to the Government.

8.7. In the event of an accident on the Department of Veterans Affairs property or involving Government personnel or property, the Contractor shall submit a report immediately to the Contracting Officer and COR in a letter form that shall include the following: (1) the time and date of occurrence; (2) the place of occurrence; (3) a list of personnel directly involves; and (4) a narrative or description of the accident to include chronological order of the accident and circumstances.

8.8. The Contractor shall not hold any discussions or release any information relating to the contract to anyone not having a direct interest in performance of this contract, without written consent of the COR with final approval of the Contracting Officer. This restriction applies to all news releases of information to the public, industry or Government agencies.

8.9. The Contractor shall not advertise information about projects performed for this contact without Government review and approval. Advertisement is considered but not limited to promotional brochures, posters, tradeshow handouts, world-wide-web- pages, magazines, newspapers and similar promotions. Past performance information for other

United States government contracts are acceptable, provided they do not contain PII.

9. VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

9.1. GENERAL

9.1.1. Contractors and contractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

9.2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

9.2.1. A contractor shall request logical (technical) or physical access to VA information and VA information systems for their employees and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

9.2.2. All contractors and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors shall be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures. Publication is available online.

9.2.3. Contract personnel who require access to national security programs shall have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

9.2.4. Custom software development and outsourced operations shall be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor shall state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

9.2.5. The contractor shall notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractors' employ. The Contracting Officer shall also be notified

immediately by the contractor prior to an unfriendly termination.

9.3. **VA INFORMATION CUSTODIAL LANGUAGE**

9.3.1. Information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor 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's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

9.3.2. VA information should not be co-mingled, if possible, with any other data on the contractor'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 shall 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 on site inspections of contractor 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.

9.3.3. Prior to termination or completion of this contract, contractor shall 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 shall 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 shall be sent to the VA Contracting Officer within 30 days of termination of the contract.

9.3.4. The contractor shall 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.

9.3.5. The contractor 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 electronic storage media for restoration in case any

electronic equipment or data used by the contractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies shall be appropriately destroyed.

9.3.6. 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 default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

9.3.7. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

9.3.8. The contractor shall store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9.3.9. The contractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

9.3.10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor shall refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

9.3.11. Notwithstanding the provision above, the contractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor is in receipt of a court order or other requests for the above mentioned information, that contractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

9.3.12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the contractor shall complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

9.4. **SECURITY INCIDENT INVESTIGATION**

9.4.1. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor has access.

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

9.4.3. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate shall notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

9.4.4. In instances of theft or break-in or other criminal activity, the contractor shall concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor and its employees shall 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 shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

9.5. **LIQUIDATED DAMAGES FOR DATA BREACH**

9.5.1. 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 processes or maintains under this contract.

9.5.2. The contractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the

risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

9.5.3. Each risk analysis shall address all relevant information concerning the data breach, including the following:

9.5.3.1. Nature of the event (loss, theft, unauthorized access);

9.5.3.2. Description of the event, including:

9.5.3.2.1. date of occurrence;

9.5.3.2.2. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

9.5.3.3. Number of individuals affected or potentially affected;

9.5.3.4. Names of individuals or groups affected or potentially affected;

9.5.3.5. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

9.5.3.6. Amount of time the data has been out of VA control;

9.5.3.7. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

9.5.3.8. Known misuses of data containing sensitive personal information, if any;

9.5.3.9. Assessment of the potential harm to the affected individuals;

9.5.3.10. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

9.5.3.11. Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

9.5.4. Based on the determinations of the independent risk analysis, the contractor shall provide credit protection services at contractor's own expense, to each affected individual consisting of the following:

9.5.4.1. Notification;

9.5.4.2. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

9.5.4.3. Data breach analysis;

9.5.4.4. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

9.5.4.5. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

9.5.4.6. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

9.6. **SECURITY CONTROLS COMPLIANCE TESTING**

9.6.1. On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the government, the contractor shall fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

9.7. **TRAINING**

9.7.1. All contractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

9.7.1.1. Sign and acknowledge understanding of and responsibilities for compliance with the *Contractor Rules of Behavior* relating to access to VA information and information systems;

9.7.1.2. Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training on the Department of Veterans Affairs Employee Education System (EES) external on-line learning website;

9.7.1.3. Successfully complete the appropriate VA privacy training and annually complete required privacy training on the Department of Veterans Affairs Employee Education System (EES) external on-line learning website; and

9.7.1.4. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

9.7.2. The contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

9.7.3. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

10. Additional requirements

10.1 If final data destruction is conducted off-site, the Contractor shall provide the facility with documented evidence of the amount and date the material was collected prior to transporting off-site.

10.2 Certificate of Destruction: A "Certificate of Destruction" shall be provided after each job. The Contractor shall complete the certificate immediately after each final destruction method is completed and return it to the COR or CO. The Certificate must state the when the documents were destroyed.

10.3. The individual performing the services shall have authority to sign the Certificate of Destruction. In the event if the contractor fails to empty a container because it was missed, upon notification by the COR or Contracting Officer (CO), the contractor shall return with 24 hours (weekdays) from the time of notified to empty the missed container; this shall be at no additional charge to the government. Contractor shall also provide proof of servicing the missed container to the COR or CO within 24 hours via email. The contractor shall only invoice for services actually performed (monthly).

10.4 OFF-SITE FINAL DESTRUCTION - If final data destruction is conducted off-site, documentation will be provided showing the reason(s) why on-site interim destruction by the vendor (prior to removal from VA custody) is not reasonably practicable?

10.5 VA Handbook 6300.1 "Records Management Procedure" shall be applicable to all shredding of information and secure information destruction. The procedure reads: "The authorized destruction of records that are classified or otherwise restricted from disclosure by statute, such as PA or Title 38 USC, must be witnessed by a Federal employee or a contractor employee. VA Directive 6371, Destruction of temporary paper

Records, is applicable to the appropriate security, protection, safeguards, and destruction of temporary paper records.

10.6 Confidentiality of material destruction: Contractor personnel shall comply with the confidentiality in the destruction of all records. Any Contractor personnel found to be reading any of the materials, secure documents, or paperwork slated for shredding shall be promptly removed from the government premises. The person(s) involved shall not be allowed to return to the VA facility for any future contract shredding services.

10.7 All Contractor vehicles utilized in this contract shall be insured and maintain current state vehicle registration. All Contractor employees shall possess a valid State Driver's license and have no traffic violations on his/her driving record. The Contractor or his/her employees while performing under this contract shall use no personal vehicles.

10.8 A VAPIHCS representative may witness and/or inspect, upon request the contractor's facilities where the materials are processed and final destruction takes place.

10.9 Insurance Requirements:

10.9.1 The Contractor is required to provide copies of proof of Worker's Compensation that complies with Federal and State Worker's Compensation and Occupational disease statues, and provide proof of General Liability Insurance, within 15 calendar days after notification of contract award.

10.9.2 In accordance with FAR Subpart 28.307-2, Liability:

10.9.3 Workers' compensation and employer's liability. Contractors are required to comply with applicable Federal and State workers' compensation and occupational disease statutes. If occupational diseases are not compensable under those statutes, they shall be covered under the employer's liability section of the insurance policy, except when contract operations are so commingled with a contractor's commercial operations that it would not be practical to require this coverage. Employer's liability coverage of at least $100,000 shall be required, except in States with exclusive or monopolistic funds that do not permit workers' compensation to be written by private carriers.

10.10 General liability:

10.10.1 The contracting officer shall require bodily injury liability insurance coverage written on the comprehensive form of policy of at least $500,000 per occurrence.

10.10.2 Property damage liability insurance coverage shall be required written on the comprehensive form of policy of at least $500,000 per occurrence.

10.11 Quality Control (QC) Plan: The contractor shall develop a QC Plan meeting the requirements of the SOW for the contracting officers review and acceptance (within 5 business days after award); and maintain the quality control program to ensure the requirements of this contract are performed in accordance with established standards. The contractor shall develop and implement procedures to identify, prevent and ensure non-recurrence of defective services. As a minimum the contractor shall develop quality control procedures (QCP) addressing the areas identified in the service summary. The contractor shall make appropriate modifications (at no additional costs to the government) and obtain acceptance of the plan by the CO. The VA shall reserve the right to determine contractor QCPs unacceptable at any time during contract performance. If a QCP is found to be unacceptable by the CO, the contractor shall be notified and resubmitted until it is found acceptable. The CO will take action to enforce the inspection of services clause requiring an inspection system acceptable to the government if an acceptable QC Plan is not submitted and approved within a reasonable time.

10.12 Quality Assurance (QA): According to the contract's inspection clause, the government will evaluate the contractor's performance under this contract. The COR is a representative of the CO and will participate in the administration of this contract. Any matter concerning a change to the scope, prices, terms, or conditions of this contract shall be referred to the CO. All services to be performed by the contractor during the period of this contract will be subject to review by the CO or COR. No additional work is allowed outside of this SOW without the written approval of the CO.

10.12.1 Service Summary:

Performance Objective	PWS Para	Acceptable Quality Level	Incentive	Disincentive
Collect/Pick-up and transport shred materials from VAPIHCS in accordance with the requirements in the Performance Work Statement	As identified in the SOW	No more than 2 valid customer complaints per month.	Favorable Contractor Performance Evaluation (CPARS)	Unfavorable Contractor performance evaluation (CPARS); Contractor Discrepancy Report (CDR), Cure Notice/Show Cause Notice/Termination of the contract.
Shred materials in accordance with NAID	As identified in the SOW	No more than 1 valid customer complaint per month.	Favorable Contractor Performance Evaluation (CPARS)	Unfavorable Contractor performance evaluation (CPARS); Contractor Discrepancy Report (CDR), Cure Notice/Show Cause Notice/Termination of the contract.

Reports and records are complete and received on time. Certificate of Destruction	As identified in the SOW	No more than 1 valid customer complaint per month.	Favorable Contractor Performance Evaluation (CPARS)	Unfavorable Contractor performance evaluation (CPARS); Contractor Discrepancy Report (CDR), Cure Notice/Show Cause Notice/Termination of the contract.

11. Technical References

11.1. VA Handbook 6300, Records and Information Management
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=429&FType=2

11.2. VA Directive 6371, Destruction of Temporary paper Records
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=523&FType=2

11.3. VA Directive 6500.6 Handbook CONTRACT SECURITY March 12, 2010
https://www.voa.va.gov/DocumentView.aspx?DocumentID=228

11.4. Health Insurance Portability and Accountability Act of 1996, Public Law 104-191
http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/index.html

11.5. VHA Privacy Policy PowerPoint Training Slides, FY10

11.6. Contractor Security Control Assessment (CSCA), May 2009

11.7. Contractor Rules of Behavior

11.8. Veterans Health Administration Business Associate Agreement (BAA)

11.9. Department of Veterans Affairs Employee Education System (EES) Required Training Courses Directions

11.10. VHA Directive 0710, Personnel Security and Suitability Program
http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1568

11.11. Homeland Security Presidential Directive – 12
http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

12. Emergency and Alarm Situations

12.1. Several smoke and heat detectors are located in the building. Do not activate fire alarm devices during non-emergency situations. The contractor shall brief his/her personnel on VA's emergency evacuation policy and ensure compliance. In the case of an emergency, the contractor's employee shall place the container(s) out of the direct

egress path (maintaining an aisle width of 44 inches or greater). The contractor shall not leave any bins or other equipment blocking fire lanes while evacuating the building. The contractor's employee shall go to the nearest stairwell and exit according to announcement instructions. During the emergency, the contractor should not attempt to move their vehicle

13. Confidentiality, Non-Disclosure and Proprietary Information:

13.1. Contractor personnel will have access to some privileged and confidential materials of the United States Government. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of the United States Government. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

13.2. The preliminary and final deliverables and all associated working papers and other material deemed relevant by VA which has been generated by the Contractor in the performance of this contract are the exclusive property of the U.S. Government and shall be submitted to the CO at the conclusion of the contract.

13.3. The Contractor shall release no information verbally or in writing, any data, the draft deliverables, the final deliverables, or any other written or printed materials pertaining to this contract. Any request for information relating to this contract presented to the Contractor shall be submitted to the CO for response.

13.4. The Contractor recognizes that in the performance of this contract the Contractor may receive or have access to sensitive information and agrees to safeguard and use the information exclusively in the performance of this contract. The Contractor shall follow all Government rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

13.5. The Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the contract then the Contractor has a responsibility to ask the Government representative.

13.6. The Contractor shall indoctrinate all personnel employed by the Contractor involved in this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive Government or patient information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information.

13.7. The Contractor shall maintain physical security at all facilities housing the activities under this contract. The Contractor shall ensure that security procedures are

defined and enforced to ensure all personnel who are provided access to sensitive data shall comply with published procedures to protect the privacy and confidentiality of such information as required by VA.

13.8. All personnel who are provided access to patient data shall comply with published procedures to protect the privacy and confidentiality of such information as required by the Department of Veterans Affairs. Contractor shall adhere to the following:

13.8.1. Controlled access to contractor premises and documentation of such.

13.8.2. Recording, monitoring, and control of access to shredding site.

13.8.3. All terminated employees are denied physical and logical access to all secure shred areas or transportation equipment/vehicles utilized in the performance of this contract.

13.8.4. The contractor must provide the capability to cancel immediately all access privileges and authorizations upon employee termination.

13.8.5. All contractor and Government employees are informed within twenty-four (24) hours of any employee termination.

13.9. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to avoid strictly any conflict of interest or even the appearance of a conflict of interest in Government-Contractor relationships.

13.10. The contractor shall follow all Government rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

13.11. All data generated shall be available to VA at all times.

14. Employee wages shall be fully burdened to include H&W in accordance with the prevailing DOL Wage Rate.

********** END OF SOW **********