



Privacy Impact Assessment
for the
**Security Activities Reporting System
(SARS)**

September 26, 2007

Contact Point

**Holly Ridgeway – Director, IT Security Division
Office of the Chief Information Officer
Office of Justice Programs
(202) 616-0653**

Reviewing Official

**Vance Hitch – Chief Information Officer
Department of Justice/Office of the Chief Information Officer
(202) 514-0507**

Approving Official

**Kenneth Mortensen – Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 353-8878**

Introduction

The primary objective of SARS is to provide the OJP Personnel Security Office with an electronic document management system that facilitates automated security processing, status tracking, allocation of resources, timely reporting, and archiving of security documents. SARS serves as a mechanism for the electronic storage of security files, enhancing the ability of authorized personnel to share information and allow the OJP Personnel Security Office to reduce the volume of paper documents.

SARS enables authorized personnel within OJP to perform the electronic capture, processing, transfer, document management, and reporting of data associated with personnel security for OJP employees, applicants for positions in and personnel under contract to OJP.

SARS is composed of the major application: Personnel Security, with three supporting applications: Scanning, Administration, and External Interfaces. These applications are integrated with an administration maintenance module, a commercial-off-the-shelf (COTS) document management system, and external interface application component to form the complete SARS.

Section 1.0

The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

SARS collects an individual's SSN, Name (Last name, First name, Middle initial), address, date of birth (DOB), gender, origin, eye color, hair color, height, weight, place of birth, position sensitivity level, office accounting code, position description number, and codes for the type of investigations conducted.

1.2 From whom is the information collected?

The individual's information is collected from OJP employees, applicants for positions in and personnel under contract to OJP, from the National Finance Center (NFC), and from the Office of Personnel Management (OPM) Personnel Investigation Processing System (PIPS).

Section 2.0

The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

Information is collected for document management and reporting of data associated with the personnel security for government employees and contractors under contract to OJP.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The E-Government Act of 2003 and the Paperwork Reduction Act (44 U.S.C. Chapter 35) authorized the collection of information in order to make it easier to access government information, improve customer services, and decrease paperwork while saving money.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Based on the information provided in Section 1.0 and 2.0, there are two identified risks associated with this information.

SARS collects personally identifiable information (PII) for background investigations on OJP employees, applicants, contractors, and outside personnel requiring access to OJP systems. The system also provides the capability for monitoring personnel security clearance processing, identifying the level of background investigation for employees; verifying the identification and security clearance status and supporting information needs.

There is the risk of unauthorized access, modification and/or misuse of SARS data by government personnel. However, the OJP Personnel Security Office personnel are required to have a Limited Background Investigation (LBI) which is a higher level of background investigation than required by the Department of Justice (DOJ). SARS is accessible by only select personnel in the OJP Personnel Security Office. Physical access to the office is also restricted to only OJP Personnel Security Office personnel; visitors are escorted throughout the area. In addition, auditing will be conducted to ensure SARS data is not subject to unauthorized access, modification and/or misuse by government personnel.

All SARS related reports and print-outs are labeled "SENSITIVE DATA – SUBJECT TO THE PROVISIONS OF FOIA/PA." All removable media that contain sensitive SARS related data is stored in a locked container in a controlled area to prevent unauthorized access, disclosure, damage, modification,

or destruction. All media containing sensitive data is destroyed, or the sensitive data is permanently removed before disposal or transfer to non-authorized persons.

SARS data is backed up on a regular basis. The SARS data is stored onsite for two weeks. Every other Wednesday, the data is sent to ArchivesOne, Inc., an offsite storage facility located in Springfield, VA. During the offsite transmission of data to ArchivesOne, Inc., SARS data can be compromised. A service agreement between Archives One, Inc. and OJP mitigates this risk. See Appendix A for the signed Service Agreement. ArchivesOne, Inc. also agrees to comply with all rules for the safety, care, and management of ArchivesOne storage facility. ArchivesOne, Inc. securely transports SARS data to a restricted access and environmentally controlled storage location.

Section 3.0

Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

SARS monitors personnel security investigations for employees, applicants, contractors, and outside personnel requiring access to OJP systems.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No. SARS does not analyze data to assist users in identifying previously unknown areas of note, concern, or pattern.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

Information collected from NFC is checked for accuracy before being imported into SARS. OPM/PIPS data is used to check for employees within SARS without an associated OPM Case Number. The OJP Personnel Security Office also performs data verification once it receives data from the individuals. The Federal Bureau of Investigation (FBI) performs name checks on all applicants by having their name in SARS checked against the FBI files. OPM/PIPS data is verified against the hard copy security forms that were initially collected from the employees.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Currently, SARS retains all current and historical data in the SARS database. Security files for government employees and contractors are kept for 5-7 years. The information is maintained and destroyed according to the principles of the Federal Records Acts and the regulations and records schedules of the National Archives and Records Administration (NARA).

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

SARS is a secure system that features user identification and password access control. The user name and password are controlled and assigned at the network level. Once a user has access to an OJP network where SARS software is installed he or she must be registered by the system administrator as a SARS user, in order to access the SARS software. Monitoring of SARS system administrator and user activities and access will be conducted within a defined periodic timeframe. In addition to system access, individual application access is controlled within SARS. Access to specific elements or subject area is also controlled by SARS security.

Section 4.0 Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of information sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Information within SARS is shared with the FBI and personnel within the OJP Personnel Security Office who have a "need to know." OJP Personnel Security Office manually exports data from SARS to Security & Emergency Planning Staff /Personnel Security Group (SEPS/PERSEG) for employee records maintenance.

4.2 For each recipient component or office, what information is shared and for what purpose?

The FBI exports and imports data with FBI Name Check System. During the security process, some applicants have their name checked against the FBI files for a match. This check indicates if the applicant has been arrested or charged with a federal crime.

4.3 How is the information transmitted or disclosed?

The FBI name check is done daily by the HR IT Specialist manually as a batch process by sending a tape cartridge of the pertinent information to FBI. The tape is processed by the FBI and returned with additional information on the subject if any was found by the check of the FBI records.

Once data is sent to the FBI for name checks a confirmation receipt e-mail from the FBI is sent to the Personnel Security Office. When the results are ready, the FBI sends a second e-mail that provides the results back to the Personnel Security Office.

The SARS application is available only to a select number of workstations within the OJP Personnel Security Office. To access the SARS Personnel Security application, the authorized user selects the Start button in the lower left corner of his or her Windows desktop, selects **Programs | SARS | SARS Personnel Security** or double-clicks the short-cut icon on his or her desktop.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Based on the information provided in Section 4.0, there are two identified risks associated with this information.

As previously mentioned, the risks of unauthorized access, modification and/or misuse of SARS data by government personnel are mitigated by restricting physical and logical access to SARS data to only select OJP Security Office personnel. Additionally, SARS data that is stored on HR IT Specialist's H:\ is encrypted.

The information collected from FBI is only accessible by the HR IT Specialist who is responsible for the hard drive. This risk is mitigated by having additional support personnel such as the HR IT Specialist's supervisor and system owner available when the HR IT Specialist is unavailable and by periodically conducting a review of the HR IT Specialist activities to ensure SARS data is not subject to unauthorized access, modification and/or misuse.

Section 5.0

External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

SARS information is shared with NFC and OPM/PIPS.

5.2 What information is shared and for what purpose?

NFC – Encrypted data is currently downloaded from the NFC every pay period (2-week intervals) to the Human Resource (HR) IT Specialists H:\ drive. The HR IT Specialist is the only person with access to the hard drive within OJP Personnel Security Office. However, this form of data protection also presents a single point of failure if the HR IT Specialist's system is compromised or unavailable. The information is downloaded to the hard-drive and written over each time new data is received but the data is not backed-up. Data from NFC is keyed by the SSN and contains detailed information about OJP employees (e.g., personal attributes: name, race, height, weight, etc., job attributes: organization, position sensitivity, dates, etc.; and payroll information: series, grade, step, pay plan, etc.). The NFC extract consists of all NFC records for OJP employees. The data serves three purposes:

- Establishes record for new employees that will require security processing.
- Provides data updates on existing employees that have been through the security process.
- Provides a mechanism for inactivating OJP employee records.

OPM/PIPS – Data is currently downloaded from the OPM/PIPS on a daily basis. Data from OPM is received in formatted flat files and is keyed by the OPM Case Number. The flat file contains three record structures: Subject Record: Subject Name, SSN, DOB, and State of Birth; Investigation Record: OPM Case information for the current case; Prior Investigation Record: OPM summary case date for the last three cases. The data serves two purposes:

- Identifies employees within SARS without an associated OPM Case Number.
- Provides case data updates on existing employee records that are currently going through the clearance process.

5.3 How is the information transmitted or disclosed?

SARS is not connected to NFC or OPM/PIPS; therefore, a MOU or SLA is not required. Data from the systems are manually imported or exported from SARS.

NFC – Encrypted data from the NFC interface traverses DOJ Metropolitan Area Network (MAN) to Enterprise Network System (ENS) to and is downloaded to the HR IT Specialist's H:\. The downloaded data file is then imported into SARS.

OPM/PIPS – The connection to OPM is established via dialup Virtual Private Network (VPN) on a stand-alone desktop computer. Data is downloaded to this machine, processed into the correct format, and transferred to a floppy diskette. The floppy diskette is hand carried to a SARS machine and the data is copied to the shared drive and then imported into SARS in a procedure similar to NFC data transfers. The files on the floppy are perpetually overwritten by the next download.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

Yes, there are agreements concerning the security and privacy of SARS data once it's shared with NFC and OPM/PIPS. OJP currently has a Memorandum of Understanding in place with the NFC and OPM/PIPS to facilitate this sharing of information between agencies.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

An external interface user training manual is available for NFC and OPM/PIPS.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

There are no provisions in place for auditing the external recipient's use of the information.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Based on the information provided in Section 5.0, there are five identified risks associated with this information.

Data from NFC can be lost during transmission to SARS and can be compromised when SARS takes ownership of the data. However, the ENS network level protection is in place to mitigate this risk. ENS employs firewalls, IDS, and virus protection mechanisms to prevent data from being compromised. In addition, SARS data is stored on the H:\ is encrypted and access to the network is controlled by an OJP network username and password.

Information downloaded from NFC to the HR IT Specialist's hard drive presents a single point of failure. If the HR IT Specialist's computer system is compromised or unavailable the information will be inaccessible. This will be mitigated by providing oversight for the HR IT Specialist. In addition, the data on the hard drive will be backed-up via the SARS Oracle database, so if the HR IT Specialist's H:\ drive

was damaged the information on the drive will be inaccessible. To mitigate these risks, the H:\ drive will be accessible by another OJP Personnel Security Office staff member.

System administrators with administrator rights have access to all H:\ drives within OJP. However, the system administrators are unable to read the SARS data since it is encrypted when downloaded from NFC. In addition, monitoring of SARS system administrator activities will be conducted.

The manual data transfer of the floppy diskette from OPM to SARS can be compromised during the manual data transfer from the diskette to SARS. However, OJP Personnel Security staff members that access SARS have a LBI and are in a restricted access locations. In addition, all removable media that contain sensitive SARS related data is stored in a locked container in a controlled area to prevent unauthorized access, disclosure, damage, modification, or destruction.

The information collected from NFC and OPM/PIPS is only accessible by the HR IT Specialist who is responsible for the hard drive. This risk is mitigated by having additional support personnel such as the HR IT Specialists supervisor and system owner available when the HR IT Specialist is unavailable and by periodically conducting a review of the HR IT Specialist activities to ensure SARS data is not subject to unauthorized access, modification and/or misuse.

Section 6.0 Notice

The following questions are directed as notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Yes. Individuals are provided with a notice to collect information and a "Personal Statement and Documentation Requirements" will be provided to the contractor/applicants prior to starting the security investigation.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. Individuals have an opportunity and right to decline to provide information and forfeit employment.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

The information in SARS is used only for the purpose specified in Section 1.0 and 2.0. Therefore, individuals consent to having their information used for the purposes stated in the security forms provided prior to them providing the information.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Any associated risks to collecting information were mitigated by receiving consent from individuals to have their information used for the purposes stated in Section 1.0 and 2.0. Data within SARS is used only to process security background investigations for those requiring access to OJP systems.

Section 7.0 Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Individuals who need access to SARS are unable to access their own information but can redress their information by using Privacy Act/ Freedom of Information Act (PA/FOIA). If a redress of their information is needed, the individual can contact the OJP Personnel Security Office to make the changes.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

The Department of Justice's FOIA/PA regulations provide those procedures at 28 C.F.R. §§ 16.3, 16.41, 16.46. The OJP Personnel Security Office handles amendment issues on a case-by-case basis. However, SARS is a tool used by the Personnel Security Office as a tracking system; therefore, individuals are unaware that records are being maintained on SARS.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

N/A. See section 7.2 above. Individuals can contact the OJP Personnel Security Office to seek amendment of their information.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Individuals can contact the OJP Personnel Security Office to contest information contained in the system. The OJP Personnel Security Office can also be contacted to discuss actions taken as a result of agency reliance on information in the system.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

The following groups will have access to the system.

- OJP SARS Administrator – The administrator of the SARS server. The person that manages the SARS server day-to-day.
- OJP SARS Users – OJP Personnel Security Office personnel.
- OJP SARS DBA Administrator – The OJP administrator of the SARS Oracle database.
- HR IT Specialist – Performs all the manual import and exports of data for SARS.
- Back-Up System Administrator – Backs-up SARS data using OJP procedures.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contractors to the OJP will not have access to SARS. Only government employees in OJP Personnel Security Office have access to SARS.

8.3 Does the system use “roles” to assign privileges to users of the system?

Yes. SARS uses “roles” to assign privileges to users of the system. The SARS Administrator establishes the roles based upon their “need to know.”

8.4 What procedures are in place to determine which users may access the system and are they documented?

All users of SARS are assigned a role by the SARS Administrator who verifies and/or validates internal user role. The system limits access only to personnel within the OJP Personnel Security Office that have a “need to know” for accessing data.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Internally, SARS users undergo a recertification process at least annually. This process includes the review and validation of all internal SARS user accounts. In addition, SARS system administrator activities will be reviewed.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

SARS monitors system access, initial creation, and subsequent modification of specific SARS data elements and user activities. The SARS history function tracks the creation and modification of SARS Personnel Security Folders (PSFs) and employment records. In addition, specific user actions and the modification of specific data elements are tracked by the SARS History function. SARS also uses Microsoft Event Viewer to monitor network events.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Training manuals are available for the Personnel Security Office system administrator and end-users. Prior to accessing SARS, users are required to review the training manuals as a form of training. Internal OJP users undergo individual Computer Security Awareness Training annually, which includes information on general system privacy.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. SARS's data is secured in accordance with FISMA requirements. The system has been certified and accredited using NIST and DOJ guidance. The last Certification & Accreditation was completed for SARS on June 02, 2006 and will be valid until June 2009. An assessment of NIST 800-53 controls is completed annually. The last assessment was completed on May 15, 2007.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

As previously mentioned, the risks of unauthorized access, modification and/or misuse of SARS data by government personnel are mitigated by restricting access to SARS data to only select OJP Security Office personnel using an OJP network username and password. Individual application access to specific elements or subject areas is controlled by the SARS application. Additionally, SARS data is stored on HR IT Specialist's H:\ is encrypted.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

SARS was also developed according to the DOJ Systems Development Life Cycle (SDLC). System goals were achieved via the DOJ SDLC guidance.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

SARS was developed in accordance with DOJ's Systems Development Life Cycle (SDLC) process.

9.3 What design choices were made to enhance privacy?

The following choices were made to enhance the privacy of SARS:

- OJP network access controls are used to enforce username password access.
- Individual SARS application access controls pertaining to specific elements or subject areas.
- Use of a stand-alone desktop computer to establish a VPN connection to NFC and OPM/PIPS.
- The encrypted storage of NFC data on the H:\ drive.

Conclusion

SARS was developed to support the activities of OJP's Personnel Security Office. SARS's primary use is to automate all security functions and improve the overall management of the security and data processes within the OJP Personnel Security Office. SARS is accessed only by a select number of personnel within the OJP Personnel Security Office.

Responsible Officials

Holly Ridgeway

Department of Justice

Appendix A - Service Agreement between ArchivesOne, Inc. and OJP

SERVICE AGREEMENT FOR Office of Justice - OJP

ArchivesOne 7726 Southern Drive Springfield, VA 22150 703 644-3500	Office of Justice - OJP 810 7th Street, NW, 8th Floor Washington, DC 20531
---	--

This is a Service Agreement ("Agreement") between ArchivesOne, Inc. ("ArchivesOne") and Office of Justice - OJP ("Depositor") for record storage services. ArchivesOne hereby agrees to accept under its management such record material ("deposits") as Depositor requests, subject to all the terms and conditions set forth herein. For the services rendered, Depositor agrees to pay ArchivesOne for storage and related service, the charges established in the schedule attached to this Agreement and made a part hereof, as may be amended from time to time, in accordance with this Agreement.

TERMS AND CONDITIONS

1. **EFFECTIVE DATE:** This Agreement becomes effective upon acceptance by both parties. Storage fees begin on the date of the first deposit of records in the facility designated by ArchivesOne.
2. **ACCEPTANCE:** No terms and conditions other than the terms and conditions contained herein shall be binding upon ArchivesOne unless accepted by it in writing. All terms and conditions contained in any prior oral or written communication, including, without limitation, Depositor's purchase order, which are different from or in addition to the terms and conditions herein are hereby rejected and shall not be binding on ArchivesOne, whether or not they would materially alter this Agreement, and ArchivesOne hereby objects thereto. All prior proposals, negotiations and representations, if any, are merged herein. In the absence of written confirmation of Depositor's acceptance of this Agreement, the utilization by Depositor of ArchivesOne storage services for a period of thirty (30) days from the date of the receipt of this Agreement or thirty (30) days from the receipt of our invoice and payment of rates then in effect shall constitute acceptance by Depositor of such pricing and the terms of this agreement unless the Depositor notifies ArchivesOne to the contrary in writing within an additional thirty (30) day period.
3. **RATES:** Depositor will pay storage charges monthly, in advance. Charges for other services will be billed monthly as they occur. All invoices are due and payable upon receipt. All sums unpaid after thirty (30) days will be subject to a service charge at the rate of one and one half per cent (1.5%) per month, or the maximum allowed by law, whichever is less, until paid in full. Any projects of significant size must be paid for in advance.
4. **CHANGES IN RATES:** The storage fees shall remain in effect throughout the first year of the original term of this Agreement and then may be revised by ArchivesOne upon thirty (30) days written notice. Rates for all other services may be revised by ArchivesOne upon thirty (30) days written notice.
5. **DEPOSITS:** All deposits for storage shall be in approved containers subject to specifications as set forth, from time to time, by ArchivesOne. All labeling, marking, indexing and sealing instructions must be in compliance with such specifications. ArchivesOne may refuse any deposits not meeting the specifications.
6. **AUTHORIZATION:** Depositor will furnish to ArchivesOne names of such agent or agents as it may authorize to have access to or to exchange or surrender records and or any contents thereof stored at ArchivesOne. Depositor will promptly notify ArchivesOne, in writing, of the termination or revocation of the authority of such agent. Depositor represents that its authorized agents have full authority to order any service for or removal of the stored material and to deliver and receive such. Such order may be given via telephone, electronically, facsimile, in writing or in person. Deposits and/or information contained in deposits, shall be delivered only to the Depositor, unless otherwise directed in writing by an authorized agent of Depositor.
7. **TRANSPORTATION:** ArchivesOne is not and shall not be deemed a contract or common carrier. Additional charges for hoisting, lowering and labor may be added to transportation costs if deposits cannot be transported in the customary manner by elevator or stairs from a reasonable accessible location.
8. **LIABILITIES:** The liability of ArchivesOne to Depositor shall be limited to damages or loss caused by its negligence and shall not exceed \$1.00 per cubic foot of storage. To the maximum extent permitted by applicable law, in no event will ArchivesOne be liable for any special, incidental, indirect, exemplary, punitive or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, procurement of substitute services or any other pecuniary

loss), even if ArchivesOne has been advised of the possibility of such damages. If Depositor intends to store material valued in excess of these limits, additional insurance should be obtained by the Depositor. Without limiting the foregoing, ArchivesOne shall not be liable for any damages due to vermin, gradual deterioration, acts of God, labor disputes, acts of war or terrorism, riots, water, fire, sprinkler leakage, or any cause beyond its control. Any claims against ArchivesOne must be made in writing describing the claim and delivered to ArchivesOne by registered mail not later than ten (10) days after any loss or damage is determined to have occurred.

9. **CONFIDENTIALITY:** ArchivesOne and its employees will hold confidential all information obtained by it with respect to Depositor and its deposits. ArchivesOne shall exercise that degree of care in safeguarding deposits entrusted to it by Depositor which a reasonable and careful company would exercise with respect to similar records of its own, provided liability of ArchivesOne to Depositor shall be limited to damages or loss in amounts set forth in Section 8 above.

10. **TITLE WARRANTY:** The Depositor warrants that it is the owner or legal custodian of the deposits and has full authority to store the deposits in accordance with the terms of this Agreement. In the event that ArchivesOne should be made party in any litigation by reason of having possession of the deposits, the Depositor agrees to indemnify and hold ArchivesOne harmless from any and all liability which may result from such possession and to pay all costs and attorneys' fees incurred by ArchivesOne in connection therewith.

11. **NONPAYMENT:** In addition to the late service charge as set forth in Section 3 above, ArchivesOne may suspend all services and refuse access to deposits by Depositor whose services remain unpaid after thirty (30) days. If Depositor fails to pay all charges for a period of one hundred twenty (120) days, ArchivesOne may, at its option, after giving notice by registered mail, either destroy the deposits, or sell any and all of the deposits and containers as scrap and apply the proceeds thereof to the sums due, without liability whatsoever to Depositor. Nothing herein shall preclude ArchivesOne from recourse to other remedies by statute or otherwise. ArchivesOne shall have a lien upon all deposits of Depositor for uncollected charges and advances hereunder. ArchivesOne shall be entitled to collect from Depositor any expenses incurred in the cost of collecting arrears, including interest and reasonable attorney's fees.

12. **TERM:** The original term of this Agreement shall be for a period of two (2) years. This Agreement shall automatically be renewed for successive terms equal to the original term, at storage and service rates in effect at time of renewal unless either party terminates this Agreement by giving the other party written notice of its election to terminate sent by certified mail, at least ninety (90) days prior to the expiration of the then existing term. For purposes of calculating annual storage fees of deposits, the volume stored shall be no less than ninety (90) percent of the initial volume or ninety (90) percent of the previous year's ending storage deposit volume, whichever is greater. Depositor will be required to pay all outstanding charges, including service charges for the current month prior to the return of the deposits to Depositor.

13. **DESTRUCTION OF RECORDS:** Upon written instructions from Depositor, ArchivesOne will destroy all or part of deposits at the then prevailing rates. Depositor releases ArchivesOne from any liability by reason of destruction of such deposits pursuant to such authority.

14. **ADDRESSES:** Any notice or redelivery of deposits to Depositor may be given or made at the address in this Agreement for Depositor until written notice of change of address has been delivered.

15. **RULES:** Depositor agrees to comply with all rules as set forth by ArchivesOne for the safety, care, and management of ArchivesOne storage facilities. Depositor agrees that it will not store narcotics, explosives, organic material which may attract vermin or insects or any other material which are otherwise illegal, hazardous, dangerous and unsafe. Depositor shall not store negotiable instruments, jewelry, check stock, ticket stock or other items that have intrinsic market value.

16. **INDEMNIFICATION:** Depositor agrees to indemnify and hold ArchivesOne harmless for all damages, including costs of defense and attorneys fees, for any and all liability which may result from possession of deposits or actions of employees and agents of Depositor hereunder.

17. **ASSIGNMENT:** ArchivesOne shall have the right to assign this Agreement, provided that the assignee assumes and agrees to be bound by the terms and conditions of this Agreement.

18. **MODIFICATION:** This Agreement may be modified only by written instrument signed by the parties hereto. The terms and conditions of this Agreement shall be binding on the parties hereto and their respective heirs, executors, administrators, successors and assigns.

19. **VALUATION OF DEPOSITS:** Depositor agrees to a maximum released value of \$1.00 per cubic foot. Any value in excess of \$1.00 may be covered by insurance purchased directly by the Depositor. Any value in excess of \$1.00 per cubic foot is solely the responsibility of Depositor.

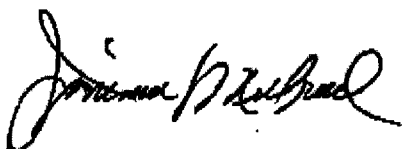
20. COUNTERPARTS: This Agreement may be executed by facsimile signature which shall be deemed to be an original and in any number of counterparts. Any party hereto may execute any such counterpart, each of which when executed and delivered shall be deemed to be an original and all of which counterparts taken together shall constitute one and the same instrument. This Agreement shall become binding when one or more counterparts taken together shall have been executed and delivered by the parties. It shall not be necessary in making proof of this Agreement or any counterpart hereof to produce or account for any of the other counterparts.

21. WARRANTIES: ArchivesOne has made no representations or warranties express or implied to Depositor except as may be contained in this Agreement.

22. GOVERNING LAW: This agreement shall be governed by and interpreted in accordance with the laws of the State of Virginia.

ArchivesOne, Inc.

Contact Name and Title Printed: Janina Mulreed, Contract Administrator



Signature:

Its duly authorized agent Date: 10/29/04

Office of Justice – OJP

Contact Name and Title Printed: _____

Signature: _____ Its duly authorized agent Date: _____

ED.3/04