



Privacy Impact Assessment  
for the

# Electronic System for Personnel (ESP)

**September 26, 2007**

**Contact Point**

**Holly Ridgeway  
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**

ESP is an automated, personnel application system, developed for OJP employees and their supervisors, to electronically prepare, review, and authorize SF-52's (requests for personnel action). The SF-52 is used to establish and maintain data pertaining to employment and payroll administration functions. The purpose of ESP is to assist users in the preparation and processing of the SF-52 for administrative action prior to submission of the data to National Finance Center (NFC) for personnel and payroll processing. ESP also manages the employee's profile, individual development plan, and training.

## **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?**

ESP automatically collects all SF-52 data from NFC which includes an employee's Name (Last name, First name), social security number (SSN), Address, Gender, Origin, date of birth (DOB), an ESP personal identification number (PIN) 4-digit number, payroll and position data. ESP also collects an employee's username and password from Active Directory Service (ADS).

### **1.2 From whom is the information collected?**

SF-52 data which includes an employees name, social security number, address, gender, origin, DOB, ESP PIN, payroll and position data is collected from NFC. Username and passwords are collected from ADS. Every two weeks ESP sends updated data to NFC which corresponds to the pay cycle.

## **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?**

ESP collects the information, as described in section, 1.1 in an effort to provide a primary means for managing the personnel action process.

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

The E-Government Act of 2002 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 four identified risks associated with this information.

Authorized users of ESP with supervisor access can view up to 100 names, SSN, series, grade, and official titles of employees that they manage. A POA&M will be created to eliminate the display of the SSN thus mitigating the risk of providing this access privilege. The SSN is not required for processing personnel action requests but if provided it can be viewed by supervisors and ESP staff including contractors (e.g., system administrators, database administrators, and Help Desk). However, information residing on ESP is not publicly accessible. The information is protected internally via the network security infrastructure. To view employee data on ESP, the employee's username and password are needed to access each individual's information. Only supervisors and system administrators can view employee's data.

ESP data is backed up on a regular basis. The ESP 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. ESP data can be compromised. A service agreement between Archives One, Inc. and OJP mitigates this risk. ArchivesOne assumes responsibility for any damage or loss of data while in their possession due to negligence. 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 ESP data to a restricted access and environmentally controlled storage location.

ESP's vendor may request information from the end-user (i.e., employee) which includes the option of providing their SSN. In the event that the employee provides this information the vendor can lose or compromise the data. ESP vendor's must follow the Contracting Officer's Technical Representative COTR's security requirements to ensure that data requested from the end-user is handled appropriately.

Lastly, there is a possible risk for this information to be used or obtained for unauthorized purposes. This risk is compounded by the fact that ESP retains all current and historical data on the system. This only increases the amount of information which could be exploited by this risk. This risk is mitigated by having only cleared government personnel utilize ESP, having the ability to establish individual accountability for system usage.

## **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.**

ESP allows OJP employees, supervisors, and managers to perform personnel management tasks. The use of ESP is typically initiated by a supervisor or manager who wants to initiate a personnel action. Personnel actions initiated by an SF-52 include reclassification and abolishment of a position; promotion, reassignment, change to lower grade, or other position change of an employee; name change; quality step increase; performance and incentive awards; denial of within-grade increase; appointment or reinstatement of a person to a position; recording and termination of a detail in excess of thirty days; recording and termination of leave without pay in excess of eighty hours, furlough, or suspension; return to duty; resignation, termination, retirement, or other separation of an employee; death; corrections; and other actions. ESP is also used for individual development plans (IDP) and training purposes.

ESP also allows management and/or users to electronically create, edit, submit, copy, delete, and maintain a history of personnel actions, create an electronic routing sheet, return personnel actions to the originator, and make comments concerning personnel actions. ESP also supports the ability to track the status of personnel actions to include training and IDP's of OJP employees.

Supervisors are allowed to view personnel action requests that pertain to the employees whom they manage. Managers with approval authority are able to create, edit, and view personnel action requests for the employees whom they directly manage.

### **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. ESP does not assist users with any type of data analysis. There is no information analysis performed on the information collected and used by ESP other than described in Section 3.1.

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

The information collected from individuals or derived from the system can be checked against the records in the Human Resource Department (HRD). The system itself does not check the accuracy of the information entered by employees and managers. However, ESP uses data from a system of record in ADS, applies it to a Personnel Action, sends it through a workflow, and then sends the record to the system of record again, which performs necessary validation. NFC verifies and validates the data provided by ESP and if any data discrepancies are present NFC will contact ESP staff to make the corrections. The verified and validated data is then sent back to NFC for personnel payroll processing.

### **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, ESP retains all current and historical data in its database. At some point, a determination will be made to archive certain history data offline. ESP does not have NARA approved retention schedule for records and information maintained. DOJ's OCIO department is working with the department retention team and NARA to develop a schedule.

### **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.**

ESP 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 and has the ESP link on their workstation he or she must be registered by the system administrator as an ESP user, in order to access the ESP software. Monitoring of ESP 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 ESP. Access to specific elements or subject area is also controlled by ESP security.

ESP audits and keeps artifacts of all aspects of documents accessed within the system. ESP logs everything from a user's opening a document to look at it, to modifications made to it, and authorizations performed, as well as any documented movement. ESP logs user information each time a comment is made; a document is returned and accommodates a comment for routing a document which logs user information.

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

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

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

ESP information is accessible by employees and supervisors of OJP. ESP staff that includes system and database administrators, and Help Desk personnel, who are contractors also have access to the system. The ESP contractors have read-only access and are unable to alter data.

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

Employees – Employees within OJP have access to their profile to review personnel action requests, request and view training, and review individual development plans.

Supervisors – Supervisors have approving authority and can view all the employees that they manage and approve personnel action requests.

Human Resource Division (HRD) – Select members of HRD have access to ESP for personnel management tasks.

### **4.3 How is the information transmitted or disclosed?**

Employees, supervisors, and managers can access ESP via a secure HTTP Intranet connection from a workstation to the server that hosts the ESP system application.

User's access the internal web servers. Upon validation, ESP users must pass an initial authentication check by the lightweight directory access protocol (LDAP) which checks a user's credentials against an authorized user list to determine whether access is granted. If access is granted, an authentication process takes place within the Oracle

database where a user profile is defined based on organizational roles and privileges created for each authorized user defined by OJP.

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

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

The only risk identified with the internal sharing of ESP information is the possible disclosure or modification of employees' information by internal government staff. The risk is mitigated by the DOJ background check which is performed on all OJP government personnel with access to ESP. OJP employees are also required to take Computer Security Annual Training (CSAT) and comply with OJP's Rules of Behavior before receiving access which informs the users of the appropriate uses of OJP systems to include ESP.

The risks identified with ESP staff including contractors (e.g., system administrators, database administrators, Help Desk) which include non-government employees (i.e., contractors) are mitigated by assigning them read-only access to ESP. Prior to accessing the system, background investigations are completed on all contractors and are only provided with access based-upon the "need to know."

In addition, ESP also has segregation of duties between the program and support offices. Roles and groups are assigned to users to ensure permissions are restricted to ensure that users have access only to data based on their role and "need to know." This is a mitigating control against the risk of unauthorized access.

## **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?**

ESP shares data with the National Finance Center (NFC), which is a unit of the Department of Agriculture (USDA), a non-DOJ Federal Agency. NFC is the conduit through which employee's profile data (e.g., Personnel Actions) flows.

### **5.2 What information is shared and for what purpose?**

ESP receives SF-52 data from NFC and then shares payroll and position information data of each employee to NFC for payroll processing.

### **5.3 How is the information transmitted or disclosed?**

The NFC/ESP interface consists of a series of steps developed to import extracted NFC data via an American Standard Code for Information Interchange (ASCII) text file. The interface eliminates the possibility of human data-entry error, thus ensuring that employee data entered, remains in the ESP system exactly as it is maintained in the NFC database. The interface passes data for all employees from NFC to ESP as described below:

The NFC/ESP interface eliminates data errors by passing employee data via an ASCII text file from the NFC to the ESP as follows:

The file is manually downloaded from NFC using Front End System Interface (FESI)

A copy of the downloaded file is placed into a directory accessible by Oracle

An Oracle stored procedure is run to import the data into the ESP Oracle database

The ESP receives data from the NFC once every two weeks. This interval corresponds to the pay cycle.

Additionally, ESP produces a file to be uploaded into NFC. These files require a secure transport between the OJP servers and NFC mainframe. Encrypted data from the NFC interface traverses DOJ Metropolitan Area Network (MAN) to Enterprise Network System (ENS).

#### **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 ESP data once it's shared with NFC. OJP currently has a Memorandum of Understanding in place with the NFC to facilitate this sharing of information between agencies. The NFC/ESP interface falls within this existing security framework to ensure that the security and privacy of the data stay intact.

Once the data is shared individual privacy is entitled under Section 552a of Title 5, U.S. Code; and U.S. Code, Title 5, Part 1, Chapter 5, Subchapter II, Sections g-1 and i-1-3 of the Privacy Act of 1974. This information is also protected by Federal and agency regulations.

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

N/A. Training is not provided to external users.

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

Yes. As stated in section 3.5, ESP audits and keeps artifacts of all aspects of documents accessed within the system. ESP logs everything from a user's opening a document to look at it, to modifications made to it, and authorizations performed, as well as any documented movement. ESP logs user information each time a comment is made, a document is returned, and accommodates a comment for routing a document which logs user information. OJP has approved and utilized a Standard Operating Procedure (SOP) for the System and User Activity Audit Logging. Audit logging of ESP is performed in accordance with this SOP.

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

Based on the information provide in Section 5.0, there were two identified risks associated with this information.

Data from ESP can be lost during transmission to NFC and can be compromised when NFC takes ownership of the data. However, there is a Memorandum of Understanding (MOU) in place between OJP and NFC to address this risk. The NFC/ESP interface falls within this existing security framework to ensure that the security and privacy of

the data stay intact. Once the data is shared individual privacy is entitled under the Privacy Act of 1974 and also protected by Federal and agency regulations.

## **Section 6.0 Notice**

The following questions are directed at 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, a form of notice is provided to individuals prior to collection of information. See Appendix B for a copy of the Privacy Act Notice from the SF-52 Personnel Action Request form.

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

Yes. The employee's SSN, origin, DOB, and gender are not required for ESP. However, the information provided from NFC is required for SF-182 and SF-52 purposes.

**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 ESP is used only for the purpose specified in Section 1.0 and 2.0. Therefore, they consent to having their information used for the purposes stated upon accessing ESP.

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

There are no associated risks identified with the privacy notice provided by ESP.

## **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?**

Employees can update only their PIN number in ESP and can change their password by contacting Help Desk. Employee's are unable to access SF-52 forms from NFC once submitted but can redress their information by using Privacy Act/ Freedom of Information Act (PA/FOIA). If changes to SF-52 data are needed the employee will need to complete and submit a new SF-52 form.

## **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.

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

N/A. ESP users are provided with an opportunity to seek amendment of their information. See section 7.2 above.

## **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.**

Once the supervisor approves the employee's information, the employee has the ability to update their ESP PIN in ESP, change their password by contacting Help Desk, and redress their information using PA/FOIA. If the employee modifies the IDP after the supervisor's approval, the approval shall be removed and the employee shall need to route the IDP back to the supervisor for approval. The supervisor shall then be able to approve the form again and submit it back to the employee.

## **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.

- Authorizer: Authorizer shall be defined as a user who is authorizing the request for personnel action (SF-52) that is to be performed on an employee or position.
- Benefits Officer: Benefits Officer shall be defined as a user designated to review SF-52s to ensure that employees receive appropriate benefits packages.

- Classifier: Classifier shall be defined as a user designated to verify the individual position and master record data on new positions or changes to an existing position before staffing may receive the SF-52.
- Payroll and Records Processing: Payroll and Records Processing shall be defined as a user designated to perform a final review prior to transmission to NFC.
- Requester: Requester shall be defined as a user who is the manager requesting a Request for Personnel Action (SF-52) to be performed on an employee or position.
- Security Officer: Security Officer shall be defined as a user designated to review SF-52s to ensure that employees and positions conform to OJP security requirements.
- Specialist: Specialists shall be defined as a user responsible for authenticating the legality of the personnel action being taken.
- Vacancy Folder: Vacancy Folder shall be defined as a user who has access to those SF-52s currently on hold.

## **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.**

Yes. ESP staff includes system administrators, database administrators, and Help Desk personnel. Contractors have read-only access to ESP. However, their access is limited to only necessary modifications to the system or when users need assistance with the application. See Appendix C for a copy of the contract.

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

Yes, the system uses “roles” to assign privileges to users of the system. The local ESP administrator establishes the roles based upon their level of authorization.

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

All users of ESP are assigned a role by the ESP system administrator who verifies and or validates internal user role assignments. The system limits access to those people who have received their User ID and Password from the ESP system administrator. These procedures can be found in ESP’s System Administrator Manual. OJP also has approved and utilizes a Standard Operating Procedure (SOP) for the Account Management process. This SOP also includes accounts created for ESP as well.

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

OJP has approved and utilizes a SOP for the Annual Re-certification process for all applicable systems to include ESP. This SOP ensures the appropriate rules and roles that have been assigned are still necessary as documented. Internally, ESP users undergo a recertification process at least annually. This process includes the review and validation of all internal ESP user accounts by the system administrator.

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

As stated in Section 5.6, ESP audits and maintains artifacts of all aspects of documents accessed within the system. ESP database administrators also have the ability to perform manual auditing on an ad hoc basis. Segregation of duties is enforced through role-based privileges and user group established by the system administrator.

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

One-on-one sessions and small “tips and tricks” sessions have been performed on an ad hoc basis. Internal OJP users undergo individual Computer Security Awareness Training (CSAT) annually, which includes information on general system privacy. Job aids are also provided to ESP users for training purposes. Employees are encouraged to become familiar with the system prior to receiving access by reading the “ESP Quick Reference Guide” and “ESP Step-by-Step Instructions”.

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

Yes, ESP’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 ESP on March 30, 2006 and will be valid until March 2009.

## **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 ESP data by government personnel are mitigated by restricting access to ESP data to only authorized users of ESP using an OJP network username and password. Individual application access to specific elements or subject areas is controlled by the ESP application.

## **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?**

Yes. ESP was developed according to the DOJ’s System Development Life Cycle (SDLC). System goals were achieved via the DOJ’s SDLC guidance.

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

ESP was developed in accordance with DOJ's SDLC. The DOJ SDLC addresses both privacy and security of the system and its data. The segregation of duties between the program and support offices in addition to role-based privileges prevent the misuse of ESP data by allowing all roles specific rights based on function and need.

## **9.3 What design choices were made to enhance privacy?**

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

- An ESP PIN is used which acts as a digital signature for additional system authorization.
- OJP network access controls are used to enforce username password access.
- Limited access privileges are granted based on roles assigned.

## **Conclusion**

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

ESP was developed to support activities related to SF-52 processing (personnel action processing), using state-of-the-art technology (e.g., electronic forms) and techniques to maximize ESP support. ESP was implemented to accomplish the following:

Allow for the electronic creation of SF-52s

Incorporate tables of value to reduce data entry requirements

Link initiation of SF-52s to employee database for automatically populating screens with personnel information

Include electronic routing capability to facilitate processing

Support the classification of positions

Provide management the capability to track requests as they are being processed

Provide management with enhanced reporting capability

## **Responsible Officials**

Holly Ridgeway

Department of Justice

# Approval Signature Page

Is/  
**Kenneth Mortensen**  
**Acting Chief Privacy and Civil Liberties Officer**  
**Department of Justice**

09/25/2007  
**Date**

<sup>FOR</sup>  
Jonathan Washington  
**Holly Ridgeway**  
**OPIT Director of Security**  
**Department of Justice**

9/25/07  
**Date**

# Appendix A: ArchivesOne Service Agreement

## 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

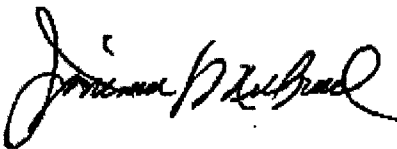
1. **EFFECTIVE DATE:** This Agreement becomes effective upon acceptance by both parties. Storage fees begin on the date of the first deposit of records in the facility designated by ArchivesOne.
2. **ACCEPTANCE:** No terms and conditions other than the terms and conditions contained herein shall be binding 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



# Appendix B – Privacy Act Statement from the SF-52 Personal Action Request Form

## Part E--Employee Resignation/Retirement

### Privacy Act Statement

You are requested to furnish a specific reason for your resignation or retirement and a forwarding address. Your reason may be considered in any future decision regarding your re-employment in the Federal service and may also be used to determine your eligibility for unemployment compensation benefits. Your forwarding address will be used primarily to mail you copies of any document you should have or any pay or compensation to which you are entitled.

This information is requested under authority of sections 301, 3301, and 8506 of title 5, U.S. Code. Sections 301 and 3301 authorize

OPM and agencies to issue regulations with regard to employment of individuals in the Federal service and their records, while section 8506 requires agencies to furnish the specific reason for termination of Federal service of the Secretary of Labor or a State agency in connection with administration of unemployment compensation programs.

The furnishing of this information is voluntary; however, failure to provide it may result in your not receiving: (1) your copies of those documents you should have; (2) pay or other compensation due you; and (3) any unemployment compensation benefits which you may be entitled.

## **Appendix C. ESP Contract**

Contact Holly Ridgeway to obtain a copy of the contract that explains the contractor's roles and responsibilities.