



START HERE
GO FURTHER
FEDERAL STUDENT AID

**Privacy Impact Assessment
for the**

***iQor/Allied Interstate
Intelligence System***

March 20, 2009

Contact Point

System Owner: Shawn Corrigan
Author: Jeff Swedberg



- 1. What information will be collected for the system?**
 - a. Information provided to us on transfer and update files from the United States Department of Education will be uploaded to the Intellione system.**
 - b. Information regarding collection activities on borrowers assigned to iQor/Allied Interstate will be collected for the system. This includes:**
 - i. Contact/location information for the subject individual or possible contact information for the subject individual, and a history of contact information on file while assigned to iQor/Allied Interstate**
 - 1. Contact information includes: phone numbers, place of employment phone and address, residential address**
 - ii. Information for persons who may know the subject individual for the purpose of locating said individual**
 - 1. Such as relatives, or previous references on file**
 - iii. Notes of attempts made to the subject individual or in an attempt to locate the subject individual**
 - iv. Information as reported by a credit bureau**
- 2. Why is this information being collected?**
 - a. This information is being collected for the collection activities of iQor/Allied Interstate's contract with the US Department of Education.**
- 3. How will FSA use this information?**
 - a. The information will be used for the following purposes, but is not limited to these:**
 - i. Contact persons we believe to be the subject individuals and verify their correct identities**
 - ii. Counsel subject individuals regarding methods to remove their accounts from default status**
 - iii. Attempt to keep paying accounts from becoming delinquent**
 - iv. In the absence of a qualifying, agreed-to repayment program, review accounts for potential involuntary collection opportunities as sanctioned by the Debt Collection Improvement Act of 1996**
 - b. Portions of this information will be updated to the FSA DMCS collection system. This includes contact information for the subject individual, notes regarding collection activities as**



- required by the contract, billing information, and employer information.
- c. The FSA routinely requests copies of the iQor/Allied Interstate system for audit purposes or to research borrower concerns.
 - d. For any other purpose as FSA or the ED contract requires.
4. Will this information be shared with any other agency or entity? If so, with which agency or agencies/entities?
- a. Information regarding collection activity will be shared with:
 - i. FSA
 - ii. PSB (small business subcontractor)
 - b. Information utilized in an attempt to secure location information, send letters, process Speedpays, or obtain information related to administrative resolutions will be shared with:
 - i. Interactive Data
 - ii. Renkim
 - iii. Lexis Nexis
 - iv. Ecommerce
 - v. Talx (Work Number)
 - vi. Central Research
5. Describe the notice or opportunities for consent that would be or are provided to individuals about what information is collected and how that information is shared with other organizations.
- a. Intentionally left blank awaiting template/further direction.
6. How will the information be secured?
- a. iQor/Allied Interstate is in the process of writing a System Security Plan (SSP) that details the security requirements and describes the security controls that are in place to meet contract requirements. A certification and accreditation process in accordance with the National Institute of Standards and Technology (NIST) "Guide for the Security Certification and Accreditation of Federal Information Systems" will be completed to validate our security controls.
 - b. Security items include, but are not limited to:
 - All data needs to be retained for a minimum of 6 months unless contracts stipulate a longer retention periods.
 - Disposal of data requires that data be rendered unreadable.
 - Cardholder data which is stored on database servers, mainframes, transfer directories and bulk data copy directories for more than 8 hours at rest needs to be encrypted.
 - All cardholder data stored on external medial must be encrypted.



- On a quarterly basis an automated extract needs to be executed to identify all cardholder data which is stored beyond retention periods.
- Operating system and database OS system support personnel need to either subscribe to a service which notifies them of the availability of security patches or must perform research of each vendor's website on a weekly basis to determine whether security patches are made available to remediate known vulnerabilities.
- Unencrypted personal information can not be sent via e-mail. WinZip Version 11 provides an acceptable form of encryption utilizing 256-bit AES encryption.
- Cardholder data received via fax machines which are transmitted to paper must be shredded immediately upon completion of data entry into payment systems. If faxes contain additional information which needs to be scanned, the cardholder data needs to be rendered unreadable. All fax machines need to be located in secured areas.
- For locations which receive fax transmissions containing cardholder data is stored on a fax server, fax transmissions need to be reviewed within one business day to identify faxes which contain cardholder data (e.g., credit card payments by debtors). Upon completion of data entry into payment systems, the fax files must be deleted from the fax server.
- All job functions which have access to application functions which allow for the display of cardholder data require approval from senior management.
- For cardholder data stored on external media, a media log needs to be established which track the movement of data. All media containing cardholder needs to be classified confidential.
- All media containing cardholder data must be sent by a secured courier or other delivery method that can be accurately tracked.
- All Audit logs need to be retained for a minimum of one year
- All locations where media containing cardholder data is stored must be secured to prevent unauthorized access.
- The retention period for records which contain cardholder data (Acct # = live PAN) is 2 years after the debtor record is in a closed status. However, the retention could be extended for records which have had activity in the last 6 months. Automated extracts need to be run on a quarterly basis to remove records which contain cardholder data.
- For credit card collection systems, credit card data needs to be removed 30 days after the payment has been received. Automated processes are to be run weekly to remove data that falls under this criterion.
- Data which is stored on tape/cartridge will be destroyed using a hammer.
- All users are required to have individual IDs.
- All passwords are required to be 8 characters alpha numeric.
- Passwords reset every 90 days.
- 15 minute of inactivity locks computers.
- User IDs and passwords are not released to new users until security materials are completed.

7. Is a system of records being created or updated with the collection of this information?

a. FSA will complete