Privacy Impact Assessment for the Ombudsman Case Tracking System (OCTSv3.0)

Date
July 19, 2006

Contact Point
System Owner: Debra Wiley
Author: Corwin K. Jennings (System Security Officer)

Federal Student Aid
U.S. Department of Education

1. What information will be collected for the system?

Information of individual users collected
Full Name
Address
SSN
Phone (Home, Work, Cell, Facsimile)
Email

2. Why is this information being collected?

(1) Information is used to establish contact with the customer seeking our assistance (*multiple contact means are desired*).
(2) To establish contact means to individual(s) relevant to finding resolution on a customer/borrower's student aid issue(s).
(3) Additionally, the customers DOB and SSN are required to match to other financial and disbursement databases to establish the financial aid history accuracy and facts associated with the borrower's claims. Summarized text entries of conversation facts detail the contact history, and eventual outcome to the customer/ borrower's student aid issue(s).

3. How will FSA use this information?

(1) To establish contact means to individual(s) relevant to finding resolution on a customer/borrower's student aid issue(s).
(2) Additionally, the customers DOB and SSN are required to match to other financial and disbursement databases to establish the financial aid history accuracy and facts associated with the borrower's claims. Summarized text entries of conversation fats detail the contact history, and eventual outcome to the customer/ borrower's student aid issue(s).

4. Will this information be shared with any other agency? If so, with which agency or agencies?

The information will be shared, when appropriate, with other government agencies focused on borrower identity verification, income verification, and payment actions.

To date, borrower/customer identification information has been shared with the Social Security Administration, the Internal Revenue Service, the Department of the Treasury.

5. Describe the notice or opportunities for consent that will be/or are provided to individuals about what information is collected and how that information is shared with others organizations.

Federal Student Aid Ombudsman posts information on our public website (http://www.ombudsman.ed.gov/) under our "Policies" link that takes the individual

to both information privacy and data security information pages that explain to the borrower how we protect their identifying data.

6. **How will the information be secured?**

The Department of Education develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

All policy and procedures may be found on ED's internal website at: http://connectED.

Federal Student Aid provides comments on departmental policy and procedures through the department's Administrative Communications System (ACS) process.

The application IDs are reviewed by the SSO quarterly. The SSO provides a list of current users to business POCs and requests them to verify who has left the project or no longer needs access to the application. The SSO will remove access as appropriate.
Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. The organization ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know changes. For SSP excerpts on controls See Below…

****

Providing Section 2.0 (Management Controls), and Section 3.0 (Operational Controls) from the SSP as follows.

2.0 MANAGEMENT CONTROLS

The Ombudsman Case Tracking System was given authorization to operate by Terri Shaw, who is the Chief Operating Officer for Federal Student Aid in November of 2003.

OCTS v3.0 was last Certified and Accredited on **November 25, 2003**.

2.1 Risk Assessment and Management

The Office of the Ombudsman "OCTS 2.0 Support System" has been classified as mission important, low risk of inflicting grave harm either upon an individual or the Department of Education if internal data should be compromised.

The Ombudsman is responsible for routine monitoring the operation of the OCTS System, reviewing the operations of her organization to ensure sound practices are being

observed by staff to protect Privacy Act data and the various forms of access to the OCTS.

An **Ombudsman Case Risk Assessment Report** (*Dated June 2002*) contains the detailed discussion of the findings for the Ombudsman Case Tracking System. The Risk Assessment Report is contained in the System Security Binder of the System Security Officer located in room 41E2, UCP-3, 830 First Street, NE, Washington, D.C. 20202-5144; a building of the U.S. Department of Education.

2.2 Review of Security Controls

The system for review is the OCTS2.0. A "Risk Assessment" of the OCTS was performed in April 2002. Results from the assessment were reported in a written document to the SSO of OCTS in June of 2002. The results/response to findings in the report are attached in figure 2 – Risk Assessment Results. The next risk assessment will be conducted in the Spring of 2005 or sooner if the system undergoes major revision.

Identified Risk (include Observation # from assessment report)	Rating	Remediation Measure	Due Date	Estimated Cost
OCTS is operational, but has not been certified and accredited.	Medium	In conjunction with FSA CSO, the VDC, and in accordance with the ED C&A Guide develop Ombudsman specific criteria that shall be used in the certification & accreditation of the Ombudsman Case Tracking System	9/30/2002	**Completed**/ June 2002
User termination and transfer procedures have not been documented.	Low	Adding user termination and transfer procedures to the Ombudsman Office Operations document.	8/30/2002	This task shall be performed by office personnel **Completed, 8/30/2002**
Users are not aware of responsibilities regarding implementation of the Contingency Plan.	Low	Inform users of their responsibilities in the event of a disaster through written documentation distributed to all Ombudsman and Intake Specialist personnel, and confirm understanding through paper or on-line sign-off on responsibilities	9/30/2002	This task shall be performed by office personnel **Completed, 11/7/2002**
A warning banner is not displayed before user login	Low	Creating a warning banner that will be presented prior to user accessing OCTSv2.0	8/30/2002	**$5,000 Completed, 9/2002** This task shall be performed by small maint. contractor for OCTS2 ROH Inc.

Figure 2

An Independent Verification & Validation Team shall perform this review. An acceptable level of risk for OCTS is MEDIUM. Medium level is defined as "an important concern, but not necessarily paramount in the organization's priorities."

2.3 Rules of Behavior

The rules governing the actions of any person working case management in the Ombudsman Office, or as a special assistant to the office, are governed by the memorandum of agreement detailed below:

The Federal Register (The Register) of Monday, December 27, 1999 sets forth the Department of Education system of records and information of the Office of the Ombudsman as required under the Privacy Act of 1974. The Register provides for disclosure of records for purposes of complaint investigation and establishes the following safeguards:

Access to and use of these records shall be limited to those persons whose official duties require access. This includes staff members of the office of The Student Loan Ombudsman, other Department offices and agents of the Department. All physical access to the sites where this system of records maintained is controlled and monitored by security personnel who check each individual entering the building for his or her employee or vision badge.

The operations of the Office of the Ombudsman and the information retained in the Ombudsman Case Tracking System, office files, customer provided information is "**Confidential**" and often highly personal. Maintenance of the integrity of the individual system of records is critical to the statutory mission of the office. Please read and sign the following confidentiality statement to confirm your understanding of and agreement to the standards of confidentiality of all Ombudsman and other Departmental staff and agents of the Office of the Ombudsman and/or the Department.

RULES OF BEHAVIOR

I promise to abide by all applicable federal statutes and regulations and hold in confidence all specific information regarding individual customers of the Office of the Ombudsman. I will not violate the confidential relationships between the Office, its customers, staff, partners and agents.

I will not remove any written customer records or copies from the office without prior written permission. Any written records I may be responsible for producing belong to the Ombudsman Office files. I accept full responsibility for maintaining the confidential and private nature of all records and information; whether in electronic or written form. I further understand that I shall discuss Ombudsman cases only with the Ombudsman Office staff, partners or agents. I will promptly report any exceptions to the Ombudsman or her designee in the Ombudsman's absence. I understand that willful failure to adhere to this agreement may result in termination.

2.4 Planning for Security in the Life Cycle

The OCTSv3.0 system is currently a closed environment system with active and passive controls permitting access to various features and capabilities based upon the users access level. Password and user id functionality shall be maintained throughout the lifecycle of the system's application software, root control software, data base revisions and communications access schemes. The lifecycle

included any re-implementation for CA, operation and maintenance of the re-implemented system, and disposal upon complete revision.

All revisions to the system shall be subject to FSA/OCIO review for security compliance, and be in compliance with the Department of Education's *Handbook for Information Technology Security System Development Life Cycle Integration Guide*.

OCTSv3.0 has no current retirement date.

2.5 Authorize Processing

The term "authorize processing" is the authorization granted by a management official for a system to process information. (Note: Some agencies refer to this authorization as **accreditation**.) Authorization provides a form of quality control and is required under OMB Circular A-130. It forces managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. By authorizing processing in a system, a manager accepts the risk associated with it. The authorizing official for this system is:

Name: Debra Wiley

Title: Ombudsman

Phone: (202) 377-3801

Both our security official and authorizing management official have security responsibilities. The security official is closer to the day-to-day operation of the system and will direct, perform, or monitor security tasks. The authorizing official will normally have general responsibility for the organization supported by the system.

Management authorization is based on an assessment of management, operational and technical controls. Since the security plan establishes the system protection requirements and documents the security controls in the system, it forms our basis for the authorization.

Below are the minimum security controls in place for OCTSv3.0:

- Technical and/or security evaluation complete.
- Risk assessment to be conducted (April 2002).
- Rules of behavior established and signed by users.
- Contingency plan developed and tested.
- Security plan developed and tested.

- A System that meets all applicable federal laws, regulations, policies, guidelines, and standards.
- In-place and planned security safeguards appear to be adequate and appropriate for the system.
- In-place safeguards are operating as intended.

3. OPERATIONAL CONTROLS (*all references to the CSC/Virtual Data Center (VDC) System Security Plan documentation can be found in the CSC/VDC Security Plan under the EDNET Public Folders in the FSA Security and Privacy/FSA Systems/VDC folder.*)

3.1 Personnel Security

All new employees to the U.S. Department of Education are subjected to a routine background check which includes a personal interview with the investigator handling their investigation. Any issues resulting from the background check are reported to the appropriate ED Management. If the individual is to be assigned to the Ombudsman Office this information would be provided on a "need-to-know" basis to the Ombudsman.

Requests for new user access to the OCTSv3.0 System are directed to the OCTS system administrator. This request is processed at the time new staff member is hired. The system administrator will assign new staff a User ID and an initial password needed to login to OCTS. Staff may change their password and are encouraged to do so every 90 days. When employees terminate employment with the Office of the Ombudsman, *the system administrator deletes all access to OCTS immediately. If an employee is administratively terminated for cause, access is denied immediately. All other out-processing actions/escort from work site actions are completed by FSA Human Resources personnel and/or Security accordingly.*

All Ombudsman Intake Specialists hold a minimum 1C clearance. Theses individuals are responsible for opening the initial case from telephone contact with a customer seeking assistance from the Ombudsman Office. The clearance is obtained during the hiring process at our partner site (Pearson, Inc.) in Iowa City, Iowa. Each individual undergoes a routine background investigation check conducted by our partner organization and the results are certified to the SSO of the OCTS. This is the basic level of clearance viewed as acceptable to serve as Ombudsman Intake Operator. All Ombudsman Case Management Specialists are cleared to 5C. Both government employees and contractor partner staff are case management specialists. All government employees have their background investigations conducted by the Department of Education, and contractor staff by the partner Pearson, Inc. These individuals are responsible for fact finding on the borrower's loan issue(s), and bringing all parties to the issue to resolution.

The **System Security Officer** is cleared to **level 6C**, and all **Technicians** who work either directly in the application/database of OCTS or provide system support or maintenance functions at Computer Systems Corporation/Virtual Data Center, Meriden, CT requiring access to host servers for the OCTS application are cleared to **level 5C**

For VDC, refer to the CSC/VDC Security Plan under the EDNET Public Folders in the FSA Security and Privacy/FSA Systems/VDC folder, under Section 3.0 (Operational Controls), subsection 3.2 (Personnel Security).

3.2 Physical and Environmental Protection

Refer to the text and diagram located in 2.2 above.

Physical and environmental security controls have been implemented to protect the virtual data center facility housing system resources, the system resources themselves, and the facilities used to support their operation. The organization responsible for providing physical security to the Ombudsman Client Tracking System is CSC Corporation.

Refer to the CSC/VDC Security Plan under the EDNET Public Folders in the FSA Security and Privacy/FSA Systems/VDC folder, under Section 3.0 (Operational Controls), subsection 3.2 (Physical and Environmental Protections).

3.2.1 Access Controls

The Computer Sciences Corporation (CSC), Virtual Data Center (VDC) is responsible for all physical security requirements associated with its providing computer support services to the Federal Student Aid organization of the U.S. Department of Education under a SLA agreement with the ED\FSA\OCIO Office. As such, only a few physical security capabilities are discussed in this section. CSC/VDC employs the latest cipher-lock technology, and password/key controls available to guard against unwanted access to the sensitive data server arrays housing the hardware and software applications comprising the Ombudsman OCTS system. Additionally, separate and distinct password/user id sign-on are required by all developers and system maintainers to gain access to the operating system environments of the supporting applications. The physical access controls restrict the entry and exit of personnel (and often equipment and media) from the office building, suite, data center, or room containing the OCTS2.0 server. All wiring supporting the server room (both electrical and data support transfer) is shielded and fully contained within the computer room with exception of the input/output connections to the physical facility. The input/output ports are covered and secured with physical locks. Backup power generation is supplied by means of an external UPS directly connected to the computer support facility. All data collected within a business day is fully backed up each evening for emergency restoration as needed. CSC-VDC provides 24x7 physical security support, with a fully manned 'HELP' operations desk, and escalation procedures in case of system or facility failures.

Refer to the CSC/VDC Security Plan under the EDNET Public Folders in the FSA Security and Privacy/FSA Systems/VDC folder, under Section 3.0 (Operational Controls), subsection 3.3 (Production Input/Output Controls and subsection 3.6 (Integrity Controls).

3.2.2 Fire Safety Controls

The Computer Sciences Corporation (CSC), Virtual Data Center (VDC) is responsible for all physical security requirements associated with its providing computer support services to the Federal Student Aid organization of the U.S. Department of Education under a SLA agreement with the ED\FSA\OCIO Office.

Refer to the CSC/VDC Security Plan under the EDNET Public Folders in the FSA Security and Privacy/FSA Systems/VDC folder, under Section 3.0 (Operational Controls), subsection 3.2 (Physical and Environmental Protections).

3.2.3 Interception of Data

There is a 'low risk' of data interception due to the use of client based software applications residing within the close loop EDNET local area network. When data is transmitted via the Internet the risk increases to MODERATE risk associated with interception, and potential dissemination of privacy act protected data.

Mobile and Portable Systems

NA.

3.3 Production, Input/Output Controls

User support. CSC/VDC provides a 24x7 help desk operation that responds to requests for general network assistance problems to problems of security incidents. The help desk operation employs a problem notification scale that elevates the involvement of management in resolving the issue as required dependent upon problem encountered. VDC uses a "check-off" process step matrix to report out the resolution to problems/issues to customers of the services. The Office of the Ombudsman is a customer.

The VDC employs "positive identification" procedures, including, but not limited to identification badges with encoded strips, computer sign-on passwords and user i.d. that enable authorized persons to access computer rooms and work terminals:

- To read, copy, and alter, and retrieve, as appropriate printed and/or electronic information.
- To pick up, receive, or deliver input and output information and media.
- To ensure accurate audit trails for receipt of sensitive inputs/outputs.
- To restrict access to input/output processes.
- To transport or mail media or printed output per established procedures.

- To establish audit trails for inventory management.
- To establish media storage vault or library physical and environmental protection controls and procedures.
- To execute procedures for sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media).
- To execute procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.
- To execute procedures for shredding, or other destructive measures for hardcopy media when no longer required.

3.4 Contingency Planning

Refer to the FSA Ombudsman Continuity of Operations Plan, Section 2.1, details restoration steps for the OCTS in the event of an emergency, and the Disaster Recovery Plan, Section 2.1, in the event service restoration must occur at a remote site. OCTS undergoes disaster recovery testing and training annually, with the last such test conducted in July 2004. Partial system restorals, with confirmation of data restoration is tested. The tests results report is contained in the SSO Security Notebook, room 41E2, UCP-3, 830 First Street, NE, Washington, D.C. 20202

The VDC is responsible for the restoration of all IT service levels to the FSA Ombudsman Office in the event of catastrophic events or long-term system failure per Task Order 11, Modification #1, dated December 8, 2000 and through FSA/CIO Service Level Agreements.

Refer to the CSC/VDC Security Plan under the EDNET Public Folders in the FSA Security and Privacy/FSA Systems/VDC folder, under Section 3.0 (Operational Controls), subsection 3.4 (Contingency Planning).

An annual disaster recovery test shall be conducted by a COMDEX facility, selected at random in the U.S. Part of the process will be to re-establish the OCTS system at a remote location. The VDC is responsible for the daily backup and storage of all system data.

The OCTS database is incrementally backed-up nightly at the Virtual Data Center beginning at 11 p.m. each day. A full back-up of the prior week data is performed at the close of each business week. In the event of a need to restore the active database, the restoration shall be through the previous business day's backup.

3.5 Application/System Hardware and Software Maintenance Controls

The VDC is responsible for all hardware and operating system applications maintenance. FSA Ombudsman application support contractor is responsible for all software upgrades, database interconnection, local application access restorations.

FSA Ombudsman utilizes the CSC/VDC change control management processes for service related outage restoration requests, and formal Siebel application software upgrades. OCTS application accessibility is the joint responsibility of the FSA Ombudsman application maintenance contractor and CSC/VDC service help desk operation. The support to be provided, as amended, is covered under the FSA/CIO SLA Agreement and the Task Order 11, Modification #1, dated December 8, 2000. See Configuration Management Plan for the Ombudsman system for a more detailed explanation of the configuration management processes for the OCTS.

Refer to the CSC/VDC Change Control Management Process in Appendix A of this document for the process steps for the VDC.

3.6 Data Integrity/Validation Controls

The small application product support vendor, currently ROH, in coordination and conjunction with the CSC Corporation, the VDC vendor, are responsible for the resolution of all data integrity and validation controls issues for the Ombudsman OCTS v3.0 System per Task Order 11, Modification #1, dated December 8, 2000 and Task Order ED-03-PO-0198 (June 2002). Data structure, manipulation and storage in the OCTS database is controlled/managed through the Siebel reference tables and structured query sets. The tables are related to each other through the "case identifier" code, and the customer demographic and history data are related at case creation to the case identifier code. The data is then arrayed into Oracle 8i data sets within pre-defined structures.

The current methodology is sufficient for the OCTS.

ENDS HERE

****

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

Yes

8. List the web addresses (known or planned) that will have a Privacy Notice.

Federal Student Aid Ombudsman Case Tracking System:
http://www.fsaombudsman.ed.gov

Federal Student Aid Ombudsman Website:
http://www.ombudsman.ed.gov