DEPARTMENT OF EDUCATION

Memorandum of Understanding

Between
The Office of Inspector General
And
Department of Education, Federal Student Aid

January 12, 2015

Version 2015.01

Revision History

Version	Release Date	Summary of Changes	Page Number	Name
2014.01	March 19, 2014	Initial Draft Issuance	N/A	N/A
2014.02	May 20, 2014	Update to Signature Authority for FSA	14	N/A
2015.01	January 12, 2015	Update to Signature Authority for FSA	14	Signature Authority

I. INTRODUCTION

The purpose of this Memorandum of Understanding (MOU) is to establish a management agreement between the Office of Inspector General (OIG) and Federal Student Aid (FSA) regarding the development, management, operation, and security of a connection between the OIG Data Analytics System (ODAS), owned by OIG, and the National Student Loan Data System, the Common Origination and Disbursement System, the Personal Identification Number System, and the Postsecondary Education Participation System, owned by FSA. This agreement governs the relationship between the two organizations regarding the above-mentioned interconnecting information technology systems, including designated managerial and technical staff. OIG and FSA will abide by the policies and procedures set forth in this agreement and the information technology policies and procedures of the Department of Education. For example, each information technology system covered by this agreement will maintain current system security plans, follow proper clearance procedures, limit access to information on a need-to-know basis, and will comply with the security requirements identified by the Department of Education.

II. AUTHORITY

The OIG enters into this MOU under the general authority of the Inspector General Act (IG Act) to promote economy, efficiency, and effectiveness in the administration of, and to prevent and detect fraud and abuse in the programs and operations of the Department. (5 U.S.C. App §2). Additionally the IG Act authorizes OIG to have access to all records or other material available to the Department that relate to its programs and operations and to request such assistance from the Department as may be necessary for carrying out the duties and responsibilities under the IG Act. (5 U.S.C. App §6)

Other laws, rules, and regulations that authorize and apply to this agreement are as follows:

- E-Government Act of 2002 including Title III Federal Information Security Management Act (FISMA), Pub. L. 107-347
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001
- Privacy Act of 1974, as amended, 5 U.S.C. §552a (Privacy Act)
- NIST SP 800-47 Security Guide for Interconnecting Information Systems, August 2002
- OMB A-130, *Management of Federal Information Resources*, November 2000

Department Guidance:

- OCIO-01: Handbook for Information Assurance Security Policy, October 2011
- OCIO-14: Handbook for Information Security Incident Response and Reporting Procedures, March 2011

- OCIO-15: Handbook for Protection of Sensitive but Unclassified Information, March 2007
- System of Records Notices
- ODAS (OIG Data Analytics System (18-10-02), 73 FR 61406 (Oct. 16, 2008) and 77 FR 28366 (May 14, 2012))
- NSLDS (National Student Loan Data System (18-11-06), 78 FR 38963 (June 28, 2013))
- COD (Common Origination and Disbursement System (18-11-02), 75 FR 59242 (Sept. 27, 2010) Department of Education (ED))
- PIN (Personal Identification Number Registration System (18-11-12), 64 FR 72400 (Dec. 27, 1999))
- PEPS (Postsecondary Education Participation System (18-11-09), 64 FR 30171 (June 4, 1999))

III. BACKGROUND

It is the intent of both parties to this MOU to address OIG's needs in reference to the above-listed FSA information technology (IT) systems for purposes of extracting and downloading specified data elements to their ODAS data warehouse on a periodic basis. OIG requires the use of these FSA IT systems to fulfill the requirements of sections (4)(a)(1), (3), and (4) of the IG Act, which require OIG to provide policy direction for and to conduct, supervise, and coordinate audits and investigations relating to programs and operations of the Department; to conduct, supervise, and coordinate activities for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud, and abuse in the programs and operations of the Department; and to conduct, supervise, or coordinate relationships between other Federal, State, and local agencies with respect to matters relating to economy and efficiency, or the prevention and detection of fraud and abuse in programs and operations of the Department or the identification and prosecution of participants in such fraud or abuse.

OIG's use of data extracted from FSA IT systems will be in furtherance of OIG's duties and responsibilities under the IG Act to conduct audits and investigations related to the programs and operations of the Department, and to conduct other activities for the purpose of promoting economy and efficiency, and preventing and detecting fraud and abuse in the programs and operations of the Department. (5 U.S.C. App. §4(a)(1) and (3)) OIG will only disclose extracted data in compliance with the Privacy Act. OIG also agrees to limit the viewing and sharing of extracted data on a need-to-know basis.

Each IT System is described below:

SYSTEM: [ODAS]
Name: OIG Data Analytics System (ODAS)

Function:	ODAS was developed to establish a central repository of data from several Department IT systems to be used to assist OIG in fulfilling its statutory responsibilities under the IG Act as set forth in "Background."
Location:	Office of Inspector General, 550 12th Street SW Room 8039, Washington, DC 20024-6122
System Owner:	Edward Slevin, CAATs Director Information Technology Audits and Computer Crime Investigations edward.slevin@ed.gov (202) 245-8183
System Manager:	Fon Lin, Supervisory IT Specialist fon.lin@ed.gov (202) 245-6184
System Security Officer:	Zachariah Wadler, Network Systems Security Administrator zachariah.waddler@ed.gov (202) 245-6535
Technical Lead:	Fon Lin, Supervisory IT Specialist fon.lin@ed.gov (202) 245-6184
Description of Data:	ODAS contains sensitive, unclassified information about individuals and entities that have applied for or received grants, contracts, loans, or payments from the Department.

ODAS will receive data extracts from the following FSA IT systems:

SYSTEM: [NSLDS]

Name:	National Student Loan Data System (NSLDS)
Function:	Central database of student aid.
Locations:	Dell Perot Systems, 2300 West Plano Parkway, Plano, TX 75075-8247 Iron Mountain, P.O. Box 294317, Lewisville, Texas 75029-4317
System Owner:	Keith Wilson, Director, Production Division Keith.wilson@ed.gov (202) 377-3591

System Manager:	Valerie Sherrer, Director, Systems Integration Division Valerie.sherrer@ed.gov (202) 377-3547
System Security Officer:	Barbara Cobbs, NSLDS ISSO Barbara.cobbs@ed.gov (202) 377-3555
Technical Lead:	Nina Colon, NSLDS Business Technical Lead Nina.colon@ed.gov (202) 377-3384
Description of Data Shared:	Sensitive, unclassified information about individuals who have applied for or received Direct Loan, Federal Family Education Loan, Federal Insured Student Loan, Federal Perkins Loan, Federal Pell Grant, and Federal Supplemental Educational Opportunity Grant funds. This data is subject to OCIO-15, Handbook for Protection of Unclassified Sensitive Information.

Extract of data from the following NSLDS tables:

1	AID_OVRPMT
2	D_ADDR
3	D_CITY
4	D_EMAIL_ADDR
5	D_EMAIL_DOMAIN
6	D_NM
7	D_POSTAL_CD
8	D_STR_ADDR
9	FINANC_PROF
10	FUNC_GP
11	GA
12	LEN
13	LEN_BR_HOL
14	LEN_BR_SVR
15	LOAN
16	LOAN_DIS
17	LOAN_RFD
18	LOC_GP
19	NSLDS_USER

20	PELL_GRT
21	PLUS_BOR
22	PLUS_BOR_LOAN
23	PLUS_BOR_NM
24	PLUS_BOR_SSN
25	PREF_SCH
26	PRSCRN_RSLT
27	SCH
28	SCH_BR
29	SCH_BR_DUNS_NO
30	STU
31	STU_BR
32	STU_DEM
33	STU_DEM_PROC_TRAN
34	STU_DEM_SUPP
35	STU_EMAIL_ADDR
36	STU_PH
37	STU_FULL_NM
38	STU_MAIL_ADDR
39	STU_NM
40	STU_SSN
41	TRAN_AUD_LOG
42	TRAN_IP
43	TRAN_LOG
44	USER_FUNC
45	IP

SYSTEM: [COD]

Name: Common Origination and Disbursement System (COD)

Function: Processes, stores, and reconciles Pell Grant and Direct Loan financial aid data.

Locations: Total Systems Services, Inc. 1600 First Ave., P.O. Box 2567, Columbus, GA 31902–2567

Affiliated Computer Services, Inc., 2429 Military Road, Suite 200, Niagara Falls, NY 14304–1551

HP Enterprise Services, COD Ancillary Services, 201 TechnaCenter Dr., Suite 300, Montgomery, AL 36117–6044

Dell Perot Systems, 2300 W. Plano Parkway, Plano, TX 75075–8427

HP Enterprise Services, D5–2B–14, 6901 Windcrest Parkway, Plano, TX 75024–8427

……

IV. COMMUNICATIONS

Frequent formal communications are essential to ensure the successful management and operation of the interconnection. The parties agree to maintain open lines of communication between designated staff at both the managerial and technical levels.

To safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit, the parties agree to provide notice of specific events within the timeframes indicated below:

- Security Incidents: System staff or technical leads who detect or otherwise learn of a security incident or a breach of personally identifiable information (PII) involving one of the systems covered by this MOU will promptly notify parties by telephone or e-mail so that the other party may take steps to determine whether its system(s) has been compromised and to take appropriate security precautions. (See Appendix A for a list of contacts.) Additionally, staff from the office experiencing the security incident will follow the incident reporting procedures set forth in OCIO-14: Handbook for Information Security Incident Response and Reporting Procedures, and will also promptly notify the Department of Education Computer Incident Response Capability (EDCIRC; edcirc@ed.gov). FSA and IG will also comply with the PII breach reporting and security requirements as required by OMB M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security into IT Investments." All parties to this MOU agree to notify each other as soon as possible, but no later than 60 minutes, after the discovery of a breach involving PII.

- Disasters and Other Contingencies: System staff who experience a disaster or other contingency that disrupts the normal operation of one or more of the systems covered by this interconnection MOU will immediately notify their designated counterparts by telephone or e-mail.

- Data Redisclosure: OIG will redisclose data only as authorized by the ODAS System of Records Notice (SORN). Any disclosure outside of what is authorized by the ODAS SORN must be mutually agreed upon by both OIG and FSA.

- Material Changes to System Configuration: Technical leads will report planned technical changes to the system architecture of one or more of the systems covered by this

interconnection MOU to their designated counterparts within a reasonable period of time before such changes are implemented. The initiating party agrees to conduct a risk assessment based on the new system architecture.

- New Interconnections: OIG will not initiate any new interconnections with third-party IT systems.
- Personnel Changes: The parties agree to provide notification of the separation or long-term absence of their respective system owner or technical lead. In addition, both parties will provide notification of any changes in point of contact information. Both parties also will provide notification of changes to user profiles, including users who resign or change job responsibilities.

V. SECURITY

All parties to this MOU will comply with all Federal requirements relating to Information Security, Information Systems Security, and privacy, including the Federal Information and Security Management Act, the E-Government Act of 2002, and NIST SP 800-53 and NIST SP 800-37. General security requirements include, but are not limited to, the following:

- Data must be protected at the Moderate system certification criticality level.
- All systems involved in the MOU have completed the security authorization process within the last three years, using the required NIST guidance, and have an Authorization to Operate (ATO) with the appropriate signatures.
- Electronic files are encrypted using the FIPS 140-2 standard and are interoperable with ED's personal identity verification logical access control card (PIV LAC) for Government Employees and support contractors authorized to have an HSPD-12 card.
- All systems participate in a continuous monitoring program.

VI. SYSTEM INTERCONNECTION

Introducing a new interconnection changes each system's technical architecture, and both parties must have a clear understanding of how systems will exchange information in order to properly incorporate changes into current and future network topologies. For this data sharing configuration, there is not a direct system interconnection but rather a sharing of a common Secure File Transfer Protocol (SFTP) server that is the collection point for the data sent by FSA and the data that is extracted by the OIG. The following provides a description of this Extract, Transform, and Load (ETL) process between ODAS and FSA IT systems covered in this agreement.

NSLDS/COD/PIN/PEPS

OIG Receives Data from NSLDS/COD/PIN/PEPS

- Data Description: Defined Data Export of NSLDS/COD/PIN/PEPS data
- Protocol used to exchange data: Secure FTP (SFTP)
- How often is data transferred: Monthly
- Describe the direction of the data flow: OIG will pull data from HPL4/SFTP[1] server

OIG Processes NSLDS/COD/PIN/PEPS Data

- Data Description: NSLDS/COD/PIN/PEPS Extract
- Protocol used to exchange data: SFTP
- How often is data transferred: Monthly

OIG Disposes of the Data

- Data Description: NSLDS/COD/PIN/PEPS Extract
- Disposal Method: When the information is no longer needed, it will be disposed in accordance with OCIO-15: Handbook for Protection of Unclassified Sensitive Information and applicable Department records schedules.
- Notification in the form of an email will be sent to FSA that specified data for the COD and PIN repositories that meet defined retention schedules has been deleted will be forwarded to the designated FSA owner.

  The referenced data received for the NSLDS and PEPS systems is a fully replace configuration and therefore will not meet this requirement.

VII. TIMELINE

This MOU is valid for three (3) years after the date of the last signature in the signature block below. At the end of the 3-year period, it will be reviewed, updated, and revalidated upon agreement by the parties. This agreement may be terminated with 30 (thirty) days advance

[1] High profile at level 4 / Secure File Transfer Protocol.

notice by either party or immediately by either party in the event of a security incident that either party believes necessitates such an action. Any changes to this MOU must be reviewed, approved, and signed by both parties.

VIII. SIGNATORY AUTHORITY

This MOU is valid for three (3) years after the last date on either signature below. At that time it will be reviewed, updated if necessary, and revalidated. This agreement may be terminated upon 30 days advanced notice by either party or in the event of a security exception that would necessitate an immediate response.

I agree to the terms and details of the MOU between the Federal Student Aid owned PEPS, NSLDS/COD/PIN and OIG.

ODAS System Owner	**FSA Systems Owner**
Edward Slevin	James W. Runcie
CAATs Director	Chief Operating Officer
Office of Inspector General	Federal Student Aid
Date: January 12, 2015	Date: _____