Appendix A through C

Appendix A
HSLS:09 Technical Review Panel (TRP) Participants

Technical Review Panel

Stephen DesJardins
Professor
Center for the Study of Higher and Postsecondary Education, School of Education; Gerald R. Ford School of Public Policy
University of Michigan
610 East University Avenue, SOE Building
Ann Arbor, MI 48129
Phone: 734-647-1984
Email: sdesj@umich.edu

Jeremy Finn
Professor
Graduate School of Education
The University at Buffalo – SUNY
422 Christopher Baldy Hall
Buffalo, NY 14260
Phone: 716-645-1126
Email: finn@buffalo.edu

Deborah Floyd
Dean and Professor
Graduate College
Florida Atlantic University
777 Glades Road, SU-80 Room 101
Boca Raton, FL 33431
Phone: 561-297-4358
Email: dfloyd@fau.edu

Robert Gonyea
Associate Director
Center for Postsecondary Research
Indiana University School of Education
1900 East Tenth Street
Bloomington, IN 47406
Phone: 812-856-3014
Email: rgonyea@indiana.edu

Vinetta Jones
School of Educatio
Howard University
2441 4th Street NW
Washington, DC 20059
Phone: 301-395-5335
Email: v_jones@howard.edu

Amaury Nora
Professor and Associate Dean for Research
College of Education and Human Development
University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249
Phone: 210-458-4112
Email: amaury.nora@utsa.edu

Kent Phillippe
Associate Vice President, Research & Student Success
American Association of Community Colleges
One Dupont Circle, NW, Suite #410
Washington, DC 20036
Phone: 202-416-4505
Email: kphillippe@aacc.nche.edu

Jeff Strohl
Director of Research
Georgetown University Center on Education and the Workforce
3300 White Haven, Suite 3200
Washington, DC 20015
Phone: 202-687-4945
Email: js787@georgetown.edu

Federal Invitees

Alicia Bolton
U.S. Department of Education, OCTAE
550 12th Street SW., Room 11108, PCP,
Washington, DC 20202
Phone: 202-245-6868
Email: alicia.bolton@ed.gov

Greg Darnieder
U.S. Department of Education, OS
Office of the Secretary
400 Maryland Avenue SW, LBJ – 7W105
Washington, DC 20202
Phone: 202-401-1367
Email: greg.darnieder@ed.gov

Kyrie Dragoo
Congressional Research Service
101 Independence Avenue, SE
LM-320
Washington, DC 20540
Phone: 202-707-4421
Email: Kdragoo@crs.loc.gov

Mark Fiegener
National Science Foundation
4201 Wilson Boulevard
Arlington, VA 22230
Phone: 703-292-4622
Email: mfiegene@nsf.gov

Rochelle (Shelly) Martinez
Office of Management and Budget
Washington, DC 20503
Phone: 202-395-3147
Email:

rochelle_w._martinez@omb.eop.gov

Ruth Neild
Deputy Director for Policy and Research
U.S. Department of Education, IES
555 New Jersey Ave, NW
Room 500e
Washington, DC 20208-5500
Phone: 202- 208-1200
Email: ruth.neild@ed.gov

Susan Rundell Singer
National Science Foundation
4201 Wilson Boulevard
Arlington, VA 22230
Phone: 703-292-8637
Email: srsinger@nsf.gov

Marsha Silverberg
U.S. Department of Education, IES
555 New Jersey Avenue NW
Room 310F
Washington, DC 20208
Phone: 202-208-7178
Email: marsha.silverberg@ed.gov

Johan Uvin
Acting Assistant Secretary
U.S. Department of Education
Office of Career, Technical and Adult Education
400 Maryland Avenue SW
Washington, DC 20202
Phone: 202-245-6332
Email: johan.uvin@ed.gov

NCES

Sharon Boivin
U.S. Department of Education, NCES
1990 K Street NW
Room 8102
Washington, DC 20006
Phone: 202-502-7627
Email: sharon.boivin@ed.gov

Peggy Carr
U.S. Department of Education, NCES
1990 K Street NW
Room 8095
Washington, DC 20006
Phone: 202-502-7321
Email: peggy.carr@ed.gov

Chris Chapman
U.S. Department of Education, NCES
1990 K Street NW
Room 9042
Washington, DC 20006
Phone: 202-502-7414
Email: chris.chapman@ed.gov

Elise Christopher
U.S. Department of Education, NCES
1990 K Street NW
Room 9030
Washington, DC 20006
Phone: 202-502-7899
Email: elise.christopher@ed.gov

Lisa Hudson
U.S. Department of Education, NCES
1990 K Street NW
Room 9036
Washington, DC 20006
Phone: 202-502-7358
Email: lisa.hudson@ed.gov

Tracy Hunt-White
U.S. Department of Education, NCES
1990 K Street NW
Room 9018
Washington, DC 20006
Phone: 202-502-7438
Email: tracy.hunt-white@ed.gov

Kashka Kubzdela
U.S. Department of Education, NCES
1990 K Street NW
Room 9014
Washington, DC 20006
Phone: 202-502-7411
Email: kashka.kubzdela@ed.gov

Marilyn Seastrom
U.S. Department of Education, NCES
1990 K Street NW
Room 9047
Washington, DC 20006
Phone: 202-502-7303
Email: marilyn.seastrom@ed.gov

Sean Simone
U.S. Department of Education, NCES
1990 K Street NW
Room 9025
Washington, DC 20006
Phone: 202-502-7367
Email: sean.simone@ed.gov

Ted Socha
U.S. Department of Education, NCES
1990 K Street NW
Room 9028
Washington, DC 20006
Phone: 202-502-7383
Email: ted.socha@ed.gov

RTI International

Melissa Cominole
RTI International
3040 East Cornwallis Road
P.O. Box 12194
Research Triangle Park, NC 27709
Phone: 919-990-8456
Email: mcominole@rti.org

Laura Fritch
RTI International
3040 East Cornwallis Road
P.O. Box 12194
Research Triangle Park, NC 27709
Phone: 919-990-8318
Email: lbfritch@rti.org

Steven Ingels
RTI International
702 13th Street NW, Suite #750
Washington, DC 20005
Phone: 202-728-2095
Email: sji@rti.org

Tiffany Mattox
RTI International
3040 East Cornwallis Road
Research Triangle Park, NC 27709
Phone: 919-485-7791
Email: tmattox@rti.org

Tim Morgan
RTI International
3040 East Cornwallis Road
P.O. Box 12194
Research Triangle Park, NC 27709
Phone: 919-485-2676
Email: timmorgan@rti.org

Dan Pratt
RTI International
3040 East Cornwallis Road
P.O. Box 12194
Research Triangle Park, NC 27709
Phone: 919-541-6615
Email: djp@rti.org

Erin Velez
RTI International
702 13th Street NW, Suite #750
Washington, DC 20005
Phone: 202-974-7879
Email: evelez@rti.org

Jamie Wescott
RTI International
3040 East Cornwallis Road
P.O. Box 12194
Research Triangle Park, NC 27709
Phone: 919-541-6990
Email: dwilson@rti.org

David Wilson
RTI International
3040 East Cornwallis Road
P.O. Box 12194
Research Triangle Park, NC 27709
Phone: 919-541-6990
Email: dwilson@rti.org

Consultants

Sandy Baum
Consultant
George Washington University and Urban Institute
161 East Chicago Avenue
#45C
Chicago, IL 60611
Phone: 518-369-3774
Email: sbaum@gwu.edu

Bruce Daniel
Sanametrix, Inc.
South Tower, Suite #200
1120 20th Street NW
Washington, DC 20036
Phone: 301-373-8344
Email: bdaniel@sanametrix.com

Dan Potter
American Institutes for Research
1000 Thomas Jefferson Street, NW
Washington, DC 20007
Phone: 202-403-6182
Email: dpotter@air.org

Appendix B
Confidentiality Procedures for Administrative Record Matching

B.1 Develop Linkages with Administrative Data Sources

Linkages will be developed with existing data sources to supplement the data collected as part of the HSLS:09 second follow-up field test and main study. NCES recognizes the great value added to the HSLS:09 data file with the addition of data from specific administrative data sources as certain data, such as college admissions test scores and information about financial aid, can only be accurately obtained from sources other than the respondent. Several NCES studies, including previous rounds of HSLS:09, the National Postsecondary Student Aid study (NPSAS), Beginning Postsecondary Student (BPS), and Baccalaureate and Beyond (B&B), have included file merges with many existing sources of valuable data, including Department of Education's (ED) Central Processing System (CPS) for Free Application for Federal Student Aid (FAFSA) data, the National Student Loan Data System (NSLDS), and the National Student Clearinghouse (NSC). For this study, we plan to perform file merges with the CPS, NSLDS, and NSC to obtain information on postsecondary enrollment and financial aid; GED, ACT, and SAT to obtain information on high school equivalency and college admissions test scores. We also plan to match the HSLS:09 sample to data provided by Catalist and Labels & Lists to obtain information on voter registration.

The Family Educational Rights and Privacy Act (FERPA) (34 CFR Part 99) allows the disclosure of information without prior consent for the purposes of HSLS:09 according to the following excerpts: 34 CFR § 99.31 asks, "Under what conditions is prior consent not required to disclose information?" and explains in 34 CFR § 99.31(a) that "An educational agency or institution may disclose personally identifiable information from an education record of a student without the consent required by §99.30 if the disclosure meets one or more" of several conditions. These conditions include, at 34 CFR § 99.31(a)(3):

> *The disclosure is, subject to the requirements of §99.35, to authorized representatives of--*
> *(i) The Comptroller General of the United States;*
> *(ii) The Attorney General of the United States;*
> *(iii) The Secretary; or*
> *(iv) State and local educational authorities.*

HSLS:09 is collecting data under the Secretary's authority. Any personally identifiable information is collected with adherence to the security protocol detailed in 34 CFR § 99.35:

> *(a)(1) Authorized representatives of the officials or agencies headed by officials listed in §99.31(a)(3) may have access to education records in connection with an audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs.*
>
> *(2) The State or local educational authority or agency headed by an official listed in §99.31(a)(3) is responsible for using reasonable methods to ensure to the greatest extent practicable that any entity or individual designated as its authorized representative—*

(i) Uses personally identifiable information only to carry out an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements related to these programs;

(ii) Protects the personally identifiable information from further disclosures or other uses, except as authorized in paragraph (b)(1) of this section; and

(iii) Destroys the personally identifiable information in accordance with the requirements of paragraphs (b) and (c) of this section.

(b) Information that is collected under paragraph (a) of this section must—

(1) Be protected in a manner that does not permit personal identification of individuals by anyone other than the State or local educational authority or agency headed by an official listed in §99.31(a)(3) and their authorized representatives, except that the State or local educational authority or agency headed by an official listed in §99.31(a)(3) may make further disclosures of personally identifiable information from education records on behalf of the educational agency or institution in accordance with the requirements of §99.33(b); and

(2) Be destroyed when no longer needed for the purposes listed in paragraph (a) of this section.

Secure Data Transfers. NCES has set up a secure data transfer system, using the NCES member site with Secure Sockets Layer (SSL) technology, described above. The contractor will use this electronic system for submitting data containing potentially identifying information (such as SSNs, names, and dates of birth of our sample members) along with their survey ID (not the same ID that is available on the restricted-use data). Before being transmitted, files will be encrypted using FIPS 140-2 validated encryption tools. Data will be received from the NCES system as well. The system requires that both parties to the transfer be registered users of the NCES Members Site and that their Members Site privileges be set to allow use of the secure data transfer service as described above. This process will be used for all file matching procedures described below, except in instances when the vendor already has a secure data transfer system in place.

B.2 File Merge with ED Central Processing System (CPS)

File merges will be performed with the CPS data containing federal student aid application information by the data collection contractor. The merge with CPS can occur at any time for any number of cases, provided that the case has an apparently valid SSN associated with it. A file will be sent to CPS and in return a large data file containing all students who applied for federal aid will be received. The data collection contractor has programs and procedures in place to prepare and submit files according to rigorous CPS standards, and to receive and process data obtained from CPS.

A file will be electronically uploaded on the FAFSA secure web-site for matching which contains SSN and the first 2 letters of the sample member’s last name (but no other information). Access to the site for the upload is restricted to authorized users who are registered and provide identification/authentication information (SSN, DOB, and personal identification number [PIN]) to the FAFSA data

site. The file is retrieved by the Central Processing System or CPS (the FAFSA contractor data system) for linkage. The linked file, containing student aid applications for matched records, is then made available to us only through a secure connection (EdConnect) which requires username and password. All CPS files will be processed, edited, and documented for inclusion on the analytic data files. All CPS files will be processed, edited, and documented for inclusion in the final restricted use file (RUF).

B.3 File Merge with National Student Loan Data System

A file merge will be conducted by the data collection contractor with the NSLDS to collect federal loan and Pell grant data. The resulting file will contain cumulative amounts for each student's entire postsecondary education enrollment. NCES has set up a secure data transfer system that uses their NCES member site and Secure Sockets Layer (SSL) technology. The system requires that both parties to the transfer be registered users of the NCES Members Site and that their Members Site privileges be set to allow use of the secure data transfer service. These privileges are set up and carefully controlled by the ED's Institute of Education Sciences (IES) NCES Chief Technology Officer (CTO), a service designed by ED/NCES specifically for the secure transfer of electronic files containing personally identifying information (i.e., data protected under the Privacy Act or otherwise posing risk of disclosure), and can be used for NCES-to-Contractor; Contractor-to-Subcontractor; Subcontractor-to-Contractor; and Contractor-to-Other-Agency data transfers. The party uploading the information onto the secure server at NCES is responsible for deleting the file(s) after the successful transfer has been confirmed. Data transfers using this system will include notification to the ED/IES, the NCES CTO, and the NCES Deputy Commissioner as well as the ED/NCES project officer. The notification will include the names and affiliations of the parties in the data exchange/transfer and the nature and approximate size of the data to be transferred. Programs have been developed to create the files for the merge and also to read the data receive. All matching processes are initiated by the data collection staff providing a file with one record per sample member to be merged.

B.4 File Merge with ACT

To obtain valuable admissions test data, a file merge will be performed with American College Testing (ACT) data by the data collection contractor. Matching of students to ACT requires Social Security number (SSN), name and date of birth to assist the data vendor in performing confirmatory data quality checks. This process will be initiated by providing a file with one record per SSN. The procedure will be to create a password-protected, encrypted file using FIPS 140-2 validated encryption tools and to upload the electronic file on the NCES server for pick-up by ACT. ACT will process the data on their database and provide the matched data on the NCES server for our secure download. This file merge will only be conducted during the full-scale study.

B.5 File Merge with College Board

To obtain SAT data, a file merge will be performed with College Board by the data collection contractor. Matching of students to SAT data requires Social Security number (SSN), name and date of birth to assist the data vendor in performing confirmatory data quality checks. This process will be initiated by providing a file

with one record per SSN. The same procedures will be used as described above for the ACT linkage: creating a password-protected, encrypted file using FIPS 140-2 validated encryption tools; uploading the electronic file on the NCES server for pick-up by the College Board. The College Board will process the data on their database and provide the matched data on the NCES server for our secure download. This file merge will only be conducted during the full-scale study.

B.6 File Merge with GED Testing Service

To obtain GED data, a file merge will be performed with the GED Testing Service by the data collection contractor. Matching of students to GED data requires Social Security number (SSN), name, and date of birth to assist the data vendor in performing confirmatory data quality checks. This process will be initiated by providing a file with one record per SSN. The same procedures will be used as described above for the ACT and SAT linkage: creating a password-protected, encrypted file using FIPS 140-2 validated encryption tools; uploading the electronic file on the NCES server for pick-up by the GED Testing Service. The GED Testing Service will process the data on their database and provide the matched data on the NCES server for our secure download. This file merge will only be conducted during the full-scale study.

B.7 File Merge with Voter Data

In an effort to gain a measure of civic participation among sample members, we will request voter registration and voting history records for HSLS:09 sample members from two private vendors of voting data. In order to perform the match, RTI will supply the vendors with names, dates of birth, and all known addresses for all sample members. After applying algorithms to identify and exclude mismatches from the resulting datasets and to reduce multiple matched records to a single best match per person, we will create variables representing whether the data indicated that a person was registered to vote in a given time period, and whether the person actually voted.

B.8 File Merge with National Student Clearinghouse

The National Student Clearinghouse will be used to obtain the *Student Tracker* data on institutions attended, enrollment dates, and degree completions for the HSLS:09 sample. The data collection contractor will first set up an account with the Clearinghouse which will enable sending and receiving of files securely over encrypted FTPS connections. The file containing sensitive student identifiers (name, date of birth, and Social Security number) will be encrypted using FIPS 140-2 validated encryption tools then submitted to the Clearinghouse using their secure FTP site. All files received by the Clearinghouse will be securely stored using FIPS 140-2 validated AES encryption, the US federal encryption standard. Matched files, containing data on enrollment dates, institution names, and degrees completed, will be returned to the data collection contractor using the same secure FTP site.

B.9 File Merge with Educational Testing System

To supplement survey and high school transcript information, ETS test score data (e.g., HiSET high school equivalency test and GRE graduate admissions test score data) will be requested. These data will be used to create summary or composite variables that will be included on the restricted-use data file and

available for analysis through NCES's online data analysis tool, PowerStats (raw data will not be released). For other studies conducted for NCES, including the National Postsecondary Student Aid Study (NPSAS), the Beginning Postsecondary Students Longitudinal Study (BPS), and prior rounds of B&B, RTI has obtained test score data for GRE, SAT, and ACT and created composite variables that have been released on restricted use files and through the online data analysis tools. To create the composite variables, we use the raw score data to create variables such as ACT/SAT subject test score quartiles. We plan to do the same for ETS score data as well.

B.10 Processing Administrative Data

The data from all of these sources, as allowed by the vendor, will be delivered for inclusion on the RUF and will be useful for creating derived variables. The derived variables will be available on PowerStats and QuickStats and both direct-pull and derived variables will be documented thoroughly.

Appendix C
Data Security Language for Vendor Contracts

Data Security Requirements

a) Contractor shall use data supplied to them by Company for the specific purpose included in the corresponding Statements of Work only.
b) Contractor will protect all data supplied to them by Company as specifically stated in Exhibit C, below.
c) Unless otherwise agreed to, Contractor will promptly and properly destroy data supplied to them by Company upon the Statement of Work completion date.

EXHIBIT C
COMPANY INFORMATION SECURITY REQUIREMENTS

A. Definitions.

"Business Contact Information" is defined as name, job title, department name, company name, business telephone, business fax number, and business email address.

"COMPANY Confidential Information" as defined in the Agreement.

"Information Processing System(s)" is defined as the individual and collective electronic, mechanical, or software components of CONTRACTOR operations that store and/or process COMPANY Confidential Information.

"Information Security Event" is defined as any situation where COMPANY Confidential Information is lost; is subject to unauthorized or inappropriate access, use, or misuse; the security, confidentiality, or integrity of the information is compromised; or the availability of CONTRACTOR Information Processing Systems is compromised by external attack.

"Security Breach" is defined as an unauthorized access to CONTRACTOR's facilities, Information Processing Systems or networks used to service, store, or access COMPANY Confidential Information, provided such unauthorized access exposes COMPANY Confidential Information or provided CONTRACTOR is required to report such unauthorized access to appropriate legal or regulatory agencies or affected COMPANY members.

"Industry best practice" is defined by the information security guidelines prepared by the PCI Security Standards Council and documented in the PCI DSS requirements as well as standards and guidelines prepared by the Federal Financial Institutions Examination Council (FFIEC)

B. Security and Confidentiality.

Before receiving, or continuing to receive, COMPANY Confidential Information, CONTRACTOR will implement and maintain an information security program that ensures: 1) COMPANY's Confidential Information and CONTRACTOR's Information Processing Systems are protected from internal and external security threats; and 2) that COMPANY Confidential Information is protected from unauthorized disclosure.

C. Security Policy.

a. Formal Security Policy. Consistent with the requirement of this Attachment, CONTRACTOR will create an information security policy that is approved by CONTRACTOR's management, published and communicated to all CONTRACTOR's employees. Such information security policy may be reviewed by COMPANY at CONTRACTOR's place of business pursuant to confidentiality obligations.

b. Security Policy Review. CONTRACTOR will review the information security policy at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

D. Asset Management.

a. Asset Inventory. CONTRACTOR shall have the ability to identify the location of all CONTRACTOR Information Processing Systems and media containing COMPANY Confidential Information.

b. Acceptable Use. CONTRACTOR will implement rules for the acceptable use of information and assets which is no less restrictive than industry best practice and consistent with the requirements of this Attachment.

c. Equipment Use While on COMPANY Premises. While on COMPANY's premises, CONTRACTOR will not connect hardware (physically or via a wireless connection) to COMPANY systems unless necessary for CONTRACTOR to perform Services under this Agreement. This hardware must be inspected / scanned by COMPANY before use.

d. Portable Devices. COMPANY Confidential Information, with the exception of Business Contact Information, may not be stored on portable devices including, but not limited to, laptops, external hard drives, Personal Digital Assistants, MP3 devices, and USB devices.

e. Personally-owned Equipment. COMPANY Confidential Information, with the exception of Business Contact Information, may not be stored on personally-owned equipment.

E. Human Resources Security.

a. Security Awareness Training. Prior to CONTRACTOR employees receiving access to COMPANY Confidential Information, they will receive security awareness training appropriate to their job function. CONTRACTOR will also ensure that recurring security awareness training is performed.

b. Removal of access Rights. The access rights of all CONTRACTOR employees to CONTRACTOR Information Processing Systems or media containing COMPANY Confidential Information will be removed immediately upon termination of their employment, contract or agreement, or adjusted upon change.

F. Physical and Environmental Security.

a. Secure Areas. CONTRACTOR will secure all areas, including loading docks, holding areas, telecommunications areas, cabling areas and off-site areas that contain Information Processing Systems or media

containing COMPANY Confidential Information by the use of appropriate security controls in order to ensure that only authorized personnel are allowed access and to prevent damage and interference. The following controls will be implemented:

i. Access will be controlled and restricted by use of a defined security perimeter, appropriate security barriers, entry controls and authentication controls. A record of all accesses will be securely maintained.

ii. All personnel will be required to wear some form of visible identification to identify them as employees, contractors, visitors, et cetera.

iii. Visitors to secure areas will be supervised, or cleared for non-escorted accessed via an appropriate background check. Their date and time of entry and departure will be recorded.

b. Environmental Security. CONTRACTOR will protect equipment from power failures and other disruptions caused by failures in supporting utilities.

G. Communications and Operations Management.

a. Protection Against Malicious Code. CONTRACTOR will implement detection, prevention, and recovery controls to protect against malicious software, which is no less than current industry best practice and perform appropriate employee training on the prevention and detection of malicious software.

b. Back-ups. CONTRACTOR will perform appropriate back-ups of CONTRACTOR Information Processing Systems and media containing COMPANY Confidential Information as required in order to ensure services and service levels described in this Statement of Work.

c. Media and Information Handling. CONTRACTOR will protect against unauthorized access or misuse of COMPANY Confidential Information contained on media by use of a media control management program and provide a copy of the program to COMPANY.

i. COMPANY input and result code data can be stored as Audit Data in a SQLServer table. All Audit Data on this SQLServer table can only be accessed for up to 180 days. After 180 days the Audit Data in the SQLServer table is automatically destroyed.

d. Media and Information Disposal. CONTRACTOR will securely and safely dispose of COMPANY Confidential Information that resides on media (including but not limited to hard copies, disks, CDs, DVDs, optical disks, USB devices, hard drives) upon the Statement of Work completion date using establishment of procedures to include, but not be limited to:

i. Disposing of COMPANY Confidential Information on mediaso that it is rendered unreadable or undecipherable, such as by burning, shredding, pulverizing or overwriting in compliance with DoD Standard 5220.22-M.

ii. Maintaining a secured disposal log that provides an audit trail of disposal activities.

iii. Purging COMPANY Confidential Information from all CONTRACTOR's physical storage mediums (filing cabinets, drawers, et cetera.) and from all Information Processing Systems, including back-up systems, within thirty (30) days of the latest occurrence of following: upon termination of this agreement; or as soon as the COMPANY Confidential Information is no longer required to perform services under this Statement of Work.

iv. Providing a Certificate of Destruction to COMPANY certifying that all COMPANY Confidential Information was purged. The certificate will be provided to COMPANY within ten (10) business days after the information was purged.

e. Exchange of Information. To protect confidentiality and integrity of COMPANY Confidential Information in transit, CONTRACTOR will:

i. Perform an inventory, analysis and risk assessment of all data exchange channels (including but not limited to FTP, HTTP, HTTPS, SMTP, modem, and fax) to identify and mitigate risks to COMPANY Confidential Information from these channels.

ii. Monitor and inspect all data exchange channels to detect unauthorized information releases.

iii. Ensure that appropriate security controls using approved data exchange channels are employed when exchanging COMPANY Confidential Information.

iv. If COMPANY Confidential Information can only be sent to CONTRACTOR electronically, then CONTRACTOR must employ industry standard encryption security measures (minimum standard of NIST's FIPS 140-2) to encrypt COMPANY Confidential Information prior to transmitting via the Internet. Otherwise, COMPANY Confidential Information can only be sent to CONTRACTOR using an encrypted (minimum standard NIST's FIPS 140-2) CD-ROM sent via courier service with a tracking number.

v. Ensure that information (including persistent cookies) about COMPANY customers, members or employees is not harvested by CONTRACTOR web pages except for purposes of this Agreement.

f. Monitoring. To protect against unauthorized access or misuse of COMPANY Confidential Information residing on CONTRACTOR Information Processing Systems, CONTRACTOR will:

i. Employ current industry best practice security controls and tools to monitor Information Processing Systems and log user activities, exceptions, unauthorized information processing activities, suspicious activities and information security events. Logging facilities and log information will be protected against tampering and unauthorized access. Logs will be kept for at least 90 days.

ii. Perform frequent reviews of logs and take necessary actions to protect against unauthorized access or misuse of COMPANY Confidential Information.

iii. At COMPANY's request, make logs available to COMPANY to assist in investigations of security breaches.

iv. Comply with all relevant legal requirements applicable to monitoring and logging activities.

v. Ensure that the clocks of all relevant information processing systems are synchronized using a national or international time source.

H. Access Control.

a. User access Management. To protect against unauthorized access or misuse of COMPANY Confidential Information residing on CONTRACTOR Information Processing Systems, CONTRACTOR will:

i. Employ a formal user registration and de-registration procedure for granting and revoking access and access rights to all CONTRACTOR Information Processing Systems.

ii. Employ a formal password management process.

iii. Perform recurring reviews of users' access and access rights to ensure that they are appropriate for the users' role.

b. User Responsibilities. To protect against unauthorized access or misuse of COMPANY Confidential Information residing on CONTRACTOR Information Processing Systems, CONTRACTOR will:

i. Ensure that CONTRACTOR Information Processing Systems users follow current security practices in the selection and use of strong passwords.

ii. Ensure that unattended equipment has appropriate protection to prohibit access and use by unauthorized individuals.

iii. Ensure that COMPANY Confidential Information contained at workstations, including but not limited to paper and on display screens is protected from unauthorized access.

c. Network access Control. access to internal, external, and public network services that allow access to CONTRACTOR Information Processing Systems shall be controlled. CONTRACTOR will:

i. Ensure that current industry best practice standard authentication mechanisms for network users and equipment are in place and updated as necessary.

ii. Ensure electronic perimeter controls are in place to protect CONTRACTOR Information Processing Systems from unauthorized access.

iii. Ensure authentication methods are used to control access by remote users.

iv. Ensure physical and logical access to diagnostic and configuration ports is controlled.

d. Operating System access Control. To protect against unauthorized access or misuse of COMPANY Confidential Information residing on CONTRACTOR Information Processing Systems, CONTRACTOR will:

i. Ensure that access to operating systems is controlled by a secure log-on procedure.

ii. Ensure that CONTRACTOR Information Processing System users have a unique identifier (user ID).

iii. Ensure that the use of utility programs that are capable of overriding system and application controls are highly restricted and tightly controlled.

iv. Ensure that inactive sessions are shut down when technically possible after a defined period of inactivity.

v. Employ restrictions on connection times when technically possible to provide additional security for high risk applications.

e. Mobile Computing and Remote Working. To protect COMPANY Confidential Information residing on CONTRACTOR Information Processing Systems from the risks inherent in mobile computing and remote working, CONTRACTOR will:

i. Perform a risk assessment to identify and mitigate risks to COMPANY Confidential Information from residing on mobile computing and remote access systems.

ii. Develop a policy, operational plans and procedures for managing mobile computing and remote access systems to ensure that COMPANY Confidential Information does not reside on or are used on these systems.

I. Information Systems Acquisition, Development and Maintenance.

a. Security of System Files. To protect CONTRACTOR Information Processing Systems and system files containing COMPANY Confidential Information, CONTRACTOR will ensure that access to source code is restricted to authorized users who have a direct need to know.

b. Security in Development and Support Processes. To protect CONTRACTOR Information Processing Systems and system files containing COMPANY Confidential Information, CONTRACTOR will:

i. Ensure that the implementation of changes is controlled by the use of formal change control procedures.

ii. Employ industry best practice security controls to minimize information leakage.

iii. Employ oversight quality controls and security management of outsourced software development.

J. Information Security Incident Management.

Reporting Information Security Events and Weaknesses. To protect CONTRACTOR Information Processing Systems and system files containing COMPANY Confidential Information, CONTRACTOR will, in the event that Contractor becomes aware of (or reasonably suspects) that any information and data obtained pursuant to the Services has been compromised in any manner, immediately notify Company via email or telephone call and follow-up on the incident in writing and provide all requested information about the event. For purposes of this obligation, "compromise" includes suspected or known incidents without limitation: (i) any unauthorized access to information and data obtained pursuant to the Services, (ii) any inadvertent disclosure of information and data obtained pursuant to the Services to any third party, (iii) any known or suspected misuse of information and data obtained pursuant to the Services by any person (even if such person was authorized to access such information or data), (iv) any suspected use of information and data obtained pursuant to the Services by any person outside of the scope of that person's authority, and (v) any known or suspected alteration of information and data obtained pursuant to the Services other than as required or permitted by this Agreement.

a. Information Security Events and Security Breaches: Contractor shall

i. Implement a process to ensure that Information Security Events and Security Breaches are reported through appropriate management channels as quickly as possible.

ii. Train all employees of information systems and services how to report any observed or suspected Information Security Events and Security Breaches.

iii. Notify COMPANY by email (JDavis@RTI.org or by phone (800-334-8571) immediately of all suspected Information Security Events and Security Breaches. Following any such event or breach, CONTRACTOR will promptly notify COMPANY as to the COMPANY Confidential Information affected and the details of the event or breach.

K. Business Continuity Management.

a. Business Continuity Management Program. In order to ensure services and service levels described in this agreement, CONTRACTOR will:

i. Develop and maintain a process for business continuity throughout the organization that addresses the information security requirements needed for the CONTRACTOR's business continuity so that the provision of products and/or services provided under the Agreement to COMPANY is uninterrupted.

ii. Identify events that can cause interruptions to business processes, along with the probability and impact of such interruptions and their consequences for information security.

iii. Develop and implement plans to maintain or restore operations and ensure availability of information at the required level and in the

required time scales following interruption to, or failure of, critical business processes and provide COMPANY a copy of the same.

iv. Test and update Business Continuity Plans regularly to ensure that they are up-to-date and effective.

L. Security Assessments.

a. Initial and Recurring Security Assessments. CONTRACTOR will permit COMPANY representatives to perform an on-site physical and logical Security Assessment of CONTRACTOR's data processing and business facilities prior to the release of COMPANY Confidential Information and each year thereafter. Security Assessments will be performed during regular business hours, at a date and time agreed to by both parties, and will not require online access to CONTRACTOR's Information Processing Systems.

b. Security Assessments Following Information Security Events and Security Breaches. Following the occurrence of an Information Security Event or Security Breach, CONTRACTOR will permit COMPANY representatives to perform an on-site physical and logical Security Assessment of CONTRACTOR's data processing and business facilities to assess the impact of the event or breach even if a Security Assessment has been completed within the year.

c. Security Assessment Findings. Upon completion of a Security Assessment, COMPANY will provide CONTRACTOR with a Security Assessment completion letter that summarizes COMPANY's Security Assessment findings. These findings may identify critical security deficiencies identified as "Mandatory" that require immediate correction before COMPANY can release, or continue to release, COMPANY Confidential Information to CONTRACTOR. CONTRACTOR will implement and continue to maintain all mutually agreed upon "Mandatory" security findings. If mutual agreement to "Mandatory" security findings cannot be reached, then these issues may be escalated using the dispute resolution provisions within this Agreement.