July 28, 2009

Thru: Kashka Kubzdela

To: Shelley Martinez, OMB

From: James Griffith

Subject: Compliance with 10 January 2008 terms of clearance for NPSAS (1850-0666 v.5 NOA).

This memorandum is submitted to comply with the 10 January 2008 terms of clearance for NPSAS (1850-0666 v.5 NOA). On that time, OMB requested an update from NCES within six months on the improvements to be made with its contractors concerning their providing PII to outside vendors for purposes of locating and tracing study respondents.

In response to OMB's request, NCES has revised the Master Service Agreements for outside vendors used by contractors to update locating information on study sample members, including the appropriate language regarding the safeguarding of personally identifying information of these individuals. The attached file includes the data security language that has been added to our contracts for the survey sample tracing/locating vendors.

18. 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, attached.
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. Protections 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.