Attachment N. NORC Data Privacy Policy

IT Capabilities & Security

IT Capabilities

NORC offers a full range of information technology, data collection, and analytic capabilities delivered in an integrated package. NORC's IT staff includes software developers, database and systems analysts, network engineers, business analysts, technical architects, and computer security experts. This group provides programming support to all NORC projects, including designing, implementing, and supporting applications for data collection, analysis, and dissemination. A dedicated Project Management Office, including many PMI certified project managers, coordinates the complicated array of tasks required to deliver IT support. NORC also features a robust IT infrastructure, including a private high-speed WAN, secure remote access systems, secure Internet, a fully automated and distributed high-capacity call center, and data centers equipped with high-performance servers and large capacity storage units.

Likewise, NORC has extensive experience designing, developing, managing, and enhancing Web sites that support a wide range of functions and content topics. Working with a variety of Web development technologies and platforms, NORC has authored many private extranet sites to support virtual communities, data dissemination portals, public Web sites, and data collection applications for federal clients ranging from the Department of Labor (DOL), Bureau of Labor Statistics (BLS), Census, Agency for Healthcare Research and Quality, the National Institutes of Health and the National Science Foundation. NORC's Web sites reflect best practices in a number of disciplines, including software and infrastructure engineering, user interface design and usability, and Section 508 compliance.

NORC IT recently released NORCSuite 3, a proprietary Case Management System (CMS) composed of a collection of software applications and databases designed to address distributed and multimode data collection projects. NORCSuite 3 is structured on web-based architecture, similar to many commercial web sites and other enterprise applications. Programmed with Java and enhanced with open-source software, NORCSuite 3 leverages universally available architecture in order to achieve scalability and extensibility. NORCSuite 3 CMS can integrate with a variety of databases and data collection tools, including custom applications developed by other projects or research companies. NORCSuite 3 is designed to also operate securely from remote locations.

In the interest of advancing our data management capacity, NORC has implemented data warehouse technology and a powerful, Web-accessible reporting and data-delivery solution for use throughout the NORC organization, as well as by our clients. These capabilities allow timely access to project data, enabling better informed project management decision making. In addition, the NORC Data Services team possesses a broad array of skills in the area of data preparation, merging, matching, linking, cleaning, and delivery. The integrated design of our data warehouse components eliminates costly, error-prone, and time-consuming tasks such as double entry, unloading, and reformatting. The team comprises experts in every major database installation and data manipulation package, including SAS and SPSS. NORC is responsible for the receipt and collection of sensitive data on a large number of projects for the federal

government and other clients. We focus on advanced methodologies to manage vast amounts of data while maintaining high security. This work is enabled by very large and expandable Storage Area Networks (SANs), relational database management systems, Internet-enabled applications, high capacity back-up infrastructure, and the use of virtual servers.

NORC's Data Services group processes electronic questionnaires fielded in various modes, including Web, phone, and personal interview, and codes, edits, and otherwise prepares the resulting data for delivery. For example, NORC combines data dictionary fields with frequency data to produce an input file for the project codebook. At the same time, the position information contained in the Data Dictionary database is used to create interim data files. This iterative, early-start approach allows NORC to rapidly produce data files that can be reviewed and modified many times before they become final. It also allows for quick review of data collection progress and identification of instrument or case-specific problems.

With an IT department of 100-plus professionals, many with industry-recognized certifications demonstrating a high degree of expertise, and a history of delivering cutting edge systems for a wide-variety of demanding clients in government and academia, NORC has the infrastructure, experience, and technological background to more than fulfill all needs outlined in this solicitation.

IT Security

Data Management and Data Security

NORC's security program is compliant with federal government regulations and can be tailored to meet the unique requirements of any particular study. NORC approaches the potential for security breaches as a grave matter and has therefore developed a multi-tiered approach to managing the various issues surrounding computer and data security. As a result, NORC complies with NIST 800.53 and FISMA regulations certified by major federal agencies through multi-year accreditations. For example, we have projects underway for the Department of Labor (DOL) as well as the Federal Reserve that have required independent audits to verify compliance. Each time we have successfully met NIST and FISMA standards.

NORC and its subcontractors will maintain the confidentiality of all data, both in flight and at rest, to which access may be gained through the contract performance. NORC and its subcontractors will not disclose this data, any interpretations or translations of this data, or derivative data to any unauthorized parties in contravention of these provisions without the prior written approval of the contracting officer. NORC understands that data collected through this contract is either the sole property of CNCS or the sole property of an institution other than the contracting parties. All of NORC's systems run on computers with automatic full disk encryption system software to protect against loss of sensitive data. NORC secures data transfer via the Internet by means of FIPS 140-2 compliant VPN. Data at rest on mobile computers or portable media are encrypted by means of using FIPS 140-2 compliant whole full disk encryption technology.

Data Management and Confidentiality:

NORC is a leader in the development of exhaustive documentation of data collection systems and processing through complex projects for such clients as the Bureau of Labor Statistics,

Health and Human Services, Treasury, NIST, USDA, and the Department of Justice. In addition, NORC, as a premier survey data collection organization, has found that the most effective method for ensuring quality in response data is to conduct regular quality checks. By examining response data as it is collected, and enforcing strict QA/QC standards, NORC identifies and resolves proactively a wide variety of data quality issues. In addition, we develop all necessary documentation to report on data errors and their resolution.

NORC requires the use of internal network data storage services to store all project-related data files. Internal network storage is provided so as to mitigate the potential of data loss due to accidents, computer equipment malfunction, failure, or human error, as well as to administer access rights surrounding the support of privacy issues that may be related to both legal and contractual obligations. Wide arrays of network security precautions are undertaken by NORC to ensure the proper storage of all project data.

These include:

- All production file servers are equipped with fault tolerant disk arrays and redundant power supplies so as to minimize the risk of losing valuable project data. These data are also protected by both surge suppression and Uninterruptible Power Supplies (UPS) as an added protective measure.
- All operating system vendors are routinely monitored by a designated NORC Information Technology (IT) infrastructure resource monitor for security patches with updates applied as necessary. Data transfers to removable media for purposes of client delivery or archival is performed on all documentation by only the IT department in order to control data formatting and assure that the media is readable by the client. This also gives the IT department the opportunity to scan the deliverables for viruses while maintaining detailed shipping manifests and receipts of all deliveries.
- All NORC authorized network users are issued an encrypted, challenge-response user-id and password which must be used to sign into each of the project applications and data areas located on the network. The user-id/password system restricts the user's access to only their specific project accounts, thereby further restricting the type of data access that is allowed for each, individual user.
- Employees are required to change their server passwords on a regular basis, so as to ensure a higher level of project security.
- The installation of any software package on a NORC computer is closely controlled. The use of any software by an employee requires a thorough review and approval process prior to installation.
- Remote access into the NORC network is performed through NORC’s firewall using both Virtual Private Network (VPN) technology and an encrypted, challenge-response technology. The primary tools used to provide this secure remote access include Juniper SSL Gateway or Citrix, depending upon the access required. A series of firewalls and packet filtering routers have been configured by the Infrastructure team so as to protect each NORC Internet Access Point, and NORC employs a dedicated IT infrastructure resource for the purpose of monitoring the LAN and WAN for signs of intrusion and other security violations. Host-based applications such as SFTP and web servers are run only on servers inside NORC's data center, and are separate from the servers that are designated to store and collect client data.

- Connectivity between all NORC sites is protected by dedicated data circuits. There is also a dedicated NORC IT resources in place for the purpose of monitoring software that proactively searches for security holes, allowing for timely corrective action.
- NORC routinely engages third-parties to conduct network security audits. A typical audit includes comprehensive attempts at network penetration from undisclosed sources and a review of policies and procedures.

Application Development

NORC adheres to the highest industry standards when developing, maintaining, and operating computer applications. NORC employs software engineering best practices with regard to the design, development, testing, and deployment of all survey instruments. The NORC Application Development Team has a diverse crew of expert programmers, business analysts, database specialists, and quality assurance personnel, all highly experienced in complex survey instrument creation. With regard to application security, all NORC applications, whether line of business or back office support, protect against unauthorized access and limit authorized access to the minimum necessary level.

Case Management and Case-Level Security

NORC employs NORCSuite Case Management System (CMS), a collection of software applications and databases designed to address distributed and multimode data collection projects. The application communicates with a Microsoft SQL Server database and can be configured to work with other database management systems. NORCSuite CMS can integrate with a variety of data collection tools, including custom tools developed by projects or research companies. The CMS manages all cases in a generic manner, tracking them through a robust set of dispositions during their lifecycle. Data-access restriction is accomplished through the use of unique case identifiers that allow the database to create a partition between response data and data that could be used to identify an individual. NORCSuite retains the flexibility to implement project specific application security practices. NORCSuite authenticates users via their web browser into a centrally managed user management system. Once authenticated, the system will allow the user access only to his or her project data and activities. Further, all user actions, including updates and additions to case information, is tracked on a per-user basis, creating a complete audit trail of activity. NORCSuite can also be used securely from remote locations. To prevent data loss through stolen equipment, all remote hardware such as laptops have secure, encryption-enabled hard drives in compliance with NIST Special Publication 800-111.

Physical Security/Facilities

With all projects, NORC takes great care to enforce a variety of physical security measures that are specifically designed to ensure that access to all confidential data is restricted to only those employees that posses both the need as well as the proper authorization to review such information. The main security precautions that NORC employs across all facilities are extensive, and are reviewed in-depth below.

- A keycard, key access, or human monitoring system (often times a combination of one or more may be used) restricts access to every NORC facility. All keycards and keys that are issued to personnel are immediately logged into a password-protected system which monitors their use. All lost or stolen keycards must be reported to the administrator immediately so that they may be deactivated. After deactivation, a new card may then be issued to the holder.
- The security of all servers and processing equipment is handled under a specific protocol. All NORC server rooms and wiring closets are located behind locked doors within the boundaries of a secure area inside the facility. Access to these areas requires the use of either a key card or a security code, which are made available only to those specific individuals that are designated to work on in these areas. All network ports on the NORC Wide Area Network (WAN) (with the exception of dial-up users) are also stored in areas of the facility that require either the use of a key, key card, or sign-in for access.
- All of NORC's data collection and processing sites are located in highly restricted areas that are readily protected by either security systems (including video cameras), the previously mentioned keycard systems, or trained guards. Only those NORC employees who have read and signed a copy of NORC's confidentiality pledge (and their escorted guests) are allowed on the premises.
- When handling and reviewing project-specific materials and data, only the staff members that are assigned to that specific project are granted access to those data and materials. The safeguards that are taken to protect this data include the use of dedicated project servers. Access to these servers can only be granted to members of the project teams by a certified member of the NORC IT staff. In addition to providing team member access to these servers, the certified staff also holds responsibility for maintaining both locked and secured filing and data storage facilities and maintaining each of the project-specific, password-protected portal sites.
- Individually identifiable data on hard copy documents is captured electronically, separated from the questionnaire, and disposed of in accordance with project-specific instructions. When physical copies of these documents must be retained or are not in use, they are stored in locked file cabinets that are accessible only to authorized project staff.

Secure Data Networks

NORC has extensive experience in adhering to secure data network standards and procedures. For example, the Racial and Ethnic Approaches to Community Health (REACH) Risk Factor Survey requires C&A certification. The REACH system is currently undergoing review by a CDC security officer. In addition, NORC has multiple NIST 800-53 Certification & Accreditations with other projects, such as National Longitudinal Survey of Youth for the Bureau of Labor Statistics (BLS).

User Rights

Once logged into NORC's application system, each user-id is assigned a rights mask that allows the user access only to well-defined, limited views of the data. Each user-id is given access only to those user interface screens that support the specific type of action the user is authorized to take.

Electronic Data Transfer External to NORC

All data used by the NORC staff is stored within and transmitted on NORC's private network and is secured as described above. Should a project obligation require that the data be electronically transmitted to or from NORC's secure private network, standard protocol dictates that encryption technology be used. Due to the variable nature of project data delivery requirements, any project that requires electronic data delivery may receive a tailored protocol. All NORC-related applications (NORC-developed or COTS) used in any environment outside of NORC's WAN are required to use digital certificates that encrypt data using Secure Sockets Layer (SSL) technology where applicable. Most applications use either Citrix or the Juniper SSL Gateway. Citrix allows us to create an encrypted session with windows-based or web-enabled applications for remote users. The Juniper SSL Gateway provides a secure encrypted session for web-enabled applications or for file transfers. The combination of the two systems provides a highly secure remote access capability with business partners and clients. It also permits highly granular security to facilitate remote access to reports and data, in addition to that of applications.

Access Control / Authentication

All user IDs and passwords that provide the user with access to NORC data are strictly controlled by NORC's IT department. All access to NORC data is automatically logged by our unified situational awareness platform for proactive alerting and audit review. As all project data are stored on the network, it is important to note that all passwords utilized are strengthened using Center for Internet Security (CIS) standards, and that the changing of passwords that protect data areas is enforced on a regular basis.

Employee Exit

Human Resources (HR) and IT coordinate so that user accounts are deactivated upon employee exit. An exit interview checklist of security-related steps is utilized by both HR and IT. NORC will notify the Contracting Officer when an employee either begins or terminates employment if that employee has access to CNCS information systems or data. If an employee is terminated for any reason, NORC will immediately disable that employee's access to information systems and data, and return to CNCS any information required under this contract.

Data Backup and Retrieval Procedures

All data that currently reside on the NORC network is backed up on tape on a nightly basis. The backup tapes are then stored in a secure, off-site location. Any information that is housed on these tapes is retrievable from the storage facility within 12 hours. All backups made for the purpose of disaster recovery have a retention period of one year. At the conclusion of a project, an archive is immediately created in strict accordance with the agreed-upon contract that was

created at the outset of the project. All archived project materials are stored off-site and are easily accessible to staff. Only a limited number of NORC's IT personnel are authorized to request the retrieval of these data tapes from the off-site location. This request for retrieval process requires a strict identification and authorization procedure.

Uninterrupted Power Supply

NORC's LAN file servers, WAN connectivity hardware, and data collection computer workstations are protected by an Uninterruptible Power Supply (UPS), thereby ensuring both orderly shutdown and data integrity maintenance in the event of power failure.

Virus Protection

In an effort to keep viruses from entering NORC systems, we have taken several preventative measures regarding virus protection. All NORC systems are protected from computer viruses by extremely robust security features and procedures. NORC's approach to limiting user access to internal network data storage services is designed specifically to minimize the possible impact of a virus that may breach NORC's virus protection software. NORC applies various daily procedures to assist in the prevention of a viral breach. Under this contract, NORC will configure its computers with the applicable United States Government Configuration Baseline (USGCB) and ensure that those computers have the latest operating system patches and virus protection software.

Paper Records Storage and Security

NORC keeps business records to meet operating, historical, research, audit, and legal requirements. The records retention policy and schedule enable NORC to ensure that valuable and legally required documents are preserved and that valueless records are only destroyed at the appropriate time.

Project Personnel Security Practices and Procedures

NORC conducts a pre-employment background investigation on each new or returning employee (if the returning employee has been gone over one year or has not previously had a background investigation conducted). Additionally, NORC may require employees transferring to a new project or different department to have a new background investigation run. All offer letters to new hires state that the offer is contingent upon satisfactory completion of a background investigation. This contingency may not be waived without the express approval of the Vice President of Human Resources. During Orientation, NORC employees are provided with NORC's Commitment to Confidentiality form, which they are required to complete as a condition of employment. NORC maintains the highest levels of confidentiality in all of our studies. At the time of hiring, the staff is explicitly trained on and required to sign a legally binding pledge upholding the confidentiality provisions established under the Privacy Act of 1974.

Incident Reporting

NORC will notify the COTR and the Corporation Chief Information Security Officer email or telephone of any incident that could potentially affect the privacy rights of individuals or which

violates any federal privacy mandates. In the event of an incident, NORC will support the Corporation's investigation and resolution of the reported incident as requested.

NORC will immediately report to the COTR and Corporation Chief Information Security Officer via email or telephone any threats or hazards to the integrity, availability and confidentiality of the Corporation Information or to the function of computer systems operated on behalf of the Corporation. Likewise, NORC will not publish or disclose in any manner the data or information to which we have access under this contract. NORC recognizes that all associated data are the sole property of CNCS and that the Contracting Office must provide prior written approval for any authorized disclosure activities, whether direct, interpreted, or derived, under this agreement. NORC will enforce these policies with any and all subcontractors we may engage.

CNCS Access to Facilities

NORC will provide CNCS, including the Corporation's Office of Inspector General, access to its and subcontractors' facilities, installations, operations, documentation, databases and personnel used in performance of the contract. Access will be provided to the extent required to carry out IT security inspection, investigation, and/or audits to safeguard against threats and hazards to the integrity, availability and confidentiality of CNCS information or to the function of computer systems operated on behalf of CNCS, and to preserve evidence of computer crime. To facilitate mandatory reviews, the NORC will ensure appropriate compartmentalization of CNCS's information, stored and/or processed, either by information systems in direct support of the contract or that are incidental to the contract.

System Security Plan and Security Authorization

IT Security Plan

NORC will develop, provide, implement and maintain an IT Security Plan which will describe the processes and procedures that will be followed to ensure the system is assessed and can obtain and maintain a security authorization. NORC will submit the IT Security Plan to the Contracting Officer and Contracting Officers Representative within four days of the contract award (*Deliverable 10)*. The IT Security Plan will include a continuous monitoring plan that includes the following elements: a configuration management process for the information system and its components; a determination of the security impact of changes to the information system and environment of operation; ongoing security control assessments in accordance with the CNCS continuous monitoring strategy; and reporting the security state of the information system to the appropriate CNCS officials. The approved IT Security Plan will be incorporated into the project contract as a compliance document.

Written proof of IT Security Authorization

Within one month of the contract award (or an agreed upon timeframe) NORC will submit written proof of an IT security authorization for acceptance by the Contracting Officer *(Deliverable 11)*. This Security Authorization will be in accordance with NIST Special Publication 800-37 and will be incorporated into the contract as a compliance document. The Security Authorization will include a final security plan, risk assessment, security test and

evaluation and disaster recovery/ continuity of operations plan. Throughout the project, NORC will comply with the accepted security authorization documentation.