Proposed Revision of Special Item Numbers (SINs) 520-16, 520-17, and 520-20 - Professional Services Schedule (PSS)

Dated July 2017

520-16: BUSINESS INFORMATION SERVICES (BIS) - Electronic and non-electronic transmission of consumer and/or business: credit reports, address verification reports, skip location reports, public information, domestic business profile, international business profile, mortgage reports, supplemental credit reference reports, bond rating, managed fund rating, institutional ranking, data processing (credit/financial) credit scoring, security freeze (lock credit file), merged credit files, business credit risk assessment, and miscellaneous business information services. Firms may provide computer software intended for BIS use and customization of reports.

520-17: RISK ASSESSMENT AND MITIGATION SERVICES - To include but not limited to: breach mitigation and forensic services, the deployment of financial risk assessment and mitigation strategies and techniques; improvement of capabilities through the reduction, identification, and mitigation of risks; detailed risk statements, risk explanations and mitigation recommendations; design and development of new business applications, processes, and procedures in response to risk assessments; and ensuring compliance with governance and regulatory requirements. Under this SIN, firms can also assist the Ordering Agency with preventive measures in protecting Personally Identifiable Information (PII) and Protected Health Information (PHI) through the evaluation of threats and vulnerabilities to PII and PHI type of information; training of Government personnel on how to prevent data breaches and identity theft; vulnerability assessments; privacy impact and policy assessments; review and creation of privacy and safeguarding policies; prioritization of threats; maintenance and demonstration of compliance; and evaluation and analysis of internal controls critical to the detection and elimination of weaknesses to the protection of PII and PHI type of information.

520-20: DATA BREACH RESPONSE AND IDENTITY PROTECTION SERVICES (IPS) - Integrated, total solution for services to provide identity monitoring and notification of Personally Identifiable Information (PII) and Protected Health Information (PHI), identity theft insurance and identity restoration services, and protect (safeguard) the confidentiality of PII and PHI. This includes the requirements found in IPS Requirements Document 1A, applicable to SIN 520-20.

NOTE 1: Additional Proposal Instructions are found in IPS Requirements Document 1B.

NOTE 2: Any firm offering this SIN will be required to provide a System Security Plan (SSP) in accordance with the template found in IPS Requirement Document 1C. The firm will also be required to submit a Firm Fixed Price per impacted individual per month pricing methodology unless otherwise defined at the Task Order level (e.g. “per product redeemed per the agreed-upon coverage period (month, year, etc.)”) covering ALL services cited in Section I of IPS Requirements Document 1A. Firms are encouraged to provide separate line item pricing for key services within this total solution SIN the firm

believes could be ordered independently (e.g., credit monitoring, restoration, etc.). This will allow the Ordering Agency to obtain only those services needed depending on level of breach. See IPS Pricing Document 2 for pricing tables.

NOTE 3: Services provided shall be performed in accordance with applicable Federal laws and policies, including the Identity Theft and Assumption Deterrence Act of 1998, as amended by Public Law 105-318, 112 Statute 3007 (Oct. 30, 1998), and implemented by 18 U.S.C. § 1028. Firms are required to adhere to all applicable Office of Management and Budget (OMB) policies including OMB Circular A-130, “Managing Federal Information as a Strategic Resource”, and any updates to OMB Memorandum M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information”.

NOTE 4: The Agency Ordering Guide can be found at www.gsa.gov/psschedule - click on “Data Breach Response and Identity Protection Services”

Identity Protection Services (IPS)
IPS Requirements Document 1A
in Support of SIN 520-20

SECTION I: DEFINITIONS

CREDIT MONITORING: is defined as the process of monitoring credit activity in order to detect any suspicious activity or changes.

CYBER INCIDENT: is defined as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on a protected Contractor information system and/or the protected information residing therein.

GOVERNMENT INFORMATION: is defined as information created, collected, processed, stored, disseminated, or disposed of by or for the Federal Government.

DATA BREACH: is defined as an incident in which personally identifiable information or protected health information has potentially been viewed, stolen, or used by an individual not authorized to do so. As defined in OMB Memorandum M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information”, a breach includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

DAYS: represent calendar days unless otherwise specified.

DATA CLEANSE: is defined as the process of detecting and correcting (or removing) corrupt or inaccurate records from a record set, table, or database. Used mainly in databases, the term refers to identifying incomplete, incorrect, inaccurate, and irrelevant parts of the data and then replacing, modifying, or deleting this dirty data or coarse data.

IDENTITY PROTECTION: is defined as establishing appropriate administrative, technical, and physical safeguards and monitoring to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

IMPACTED INDIVIDUALS: to be defined at the Task Order level.

PERSONALLY IDENTIFIABLE INFORMATION (PII) is defined as information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.

PROTECTED CONTRACTOR INFORMATION SYSTEM: is defined as an information

system that is owned or operated by or for a Contractor and that processes, stores, or transmits protected information. Protected information is defined as information provided to the Contractor by or on behalf of the Federal Government or provided by impacted individuals in connection with the performance of the contract; or collected, received, transmitted, developed, used, or stored by or on behalf of the Contractor in support of the performance of the contract.

PROTECTED HEALTH INFORMATION (PHI) is defined in detail by 45 C.F.R.160.103 as: any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Records is defined as all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. (44 U.S.C. 3301)

SYSTEM SECURITY PLAN

In order to provide services under SIN 520-20, the Contractor shall be required to submit a “moderate impact level” System Security Plan (SSP) at the GSA contract level. This plan will be prepared in accordance with the template provided under IPS Requirements Document 1C (attached) and follow the security requirements outlined in NIST SP 800-53 (latest revision).

The Contractor will be required to be knowledgeable of the requirements of both NIST SP 800-53 and NIST SP 800-171 (latest revision) as determined at the Task Order level.

Contractors with PHI and certain PII as determined by FIPS 199 classification may be required to provide a “high impact level” SSP and/or additional “compensating” controls at the Task Order level that requires additional controls to be implemented.

If no specific plan is identified at the Task Order level, the Contractor will be required to adhere to the template required by GSA.

If any changes/updates are required to the approved System Security Plan at the Task Order

level, the Contractor will be required to submit an updated plan to the Ordering Agency designee and provide a copy of that revised plan to the GSA IPS Program Manager upon approval by the Ordering Agency.

SECURITY AND SECURITY RELATED REPORTING REQUIREMENTS:

The Contractor's invoicing, billing, and other financial/administrative records/databases may not store or include any sensitive Government information, such as PII or PHI, that was created, obtained, or provided during the performance of the Task Order. It is acceptable to list the names, titles and contact information for the Ordering Contracting Officer, or other Ordering Agency personnel associated with the administration of the Task Order in the invoices as needed.

The Ordering Agency Contracting Officer's approval is required prior to engaging in any contractual relationship in support of any order requiring the disclosure of information, documentary material and/or records generated under, or relating to, work performed under the Task Order. The Contractor (and its subcontractor, partners, etc.) is required to abide by Government and individual Ordering Agency guidance for protecting sensitive and protected information.

POST AWARD DATA INCIDENT REPORTING PROCEDURES:

The Contractor must report ALL incidents involving PII and/or PHI breaches according to the notification requirements for data classification to the Ordering Agency designated official within one (1) hour of the initial discovery. This includes all incidents involving PII and/or PHI in electronic or physical form and should not distinguish between suspected and confirmed breaches. If, during performance of any Task Order awarded, the Contractor suffers a suspected and/or actual loss or compromise of PII or PHI, the Contractor is required to provide a written report to the designated Ordering Agency official within 24 hours of a suspected and/or actual loss or compromise of PII or PHI containing the following information:

a) Narrative, detailed description of the events surrounding the suspected loss/compromise
b) Date, time, and location of the incident
c) Type of information lost or compromised
d) Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment
e) Contractor's assessment of the likelihood that the information compromised can be recovered
f) Names of person(s) involved, including victim, Contractor employee/subcontractor and any witnesses
g) Cause of the incident and whether the company's security plan was followed or not, and which specific provisions were not followed
h) Actions that have been or will be taken to minimize damage and/or mitigate further compromise
i) Require Contractors and subcontractors to properly encrypt PII and PHI using FIPS 140-2 Security Requirements for Cryptographic Modules**[1]** and refrain from practices that violate agency PII and PHI protection policies

[1] Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules (NIST, December 2002)

GOVERNMENT PROVIDED INFORMATION:

As required and applicable, for each Task Order placed, the Contractor will be provided with a list of the names and addresses of all individuals affected who are eligible for identity theft services to whom notices must be mailed by the Contractor. The Ordering Office may require Contractor services to research missing point of contact information on impacted individuals as an additional service (Skip Tracing). The Ordering Office issuing the Task Order will define method of notification, content of notification, and additional PII or PHI about affected individuals whose addresses are not known or for whom notification by mail has failed. Additional notification by certified or registered mail will be made to affected individuals for which a PIN number has not been claimed within two weeks. Any information that pertains to PII and PHI will be held to the same standards as Federally Mandated in the Privacy Act of 1974, the E-Government Act of 2002, Federal Information Security Modernization Act (FISMA) of 2014, Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 and any other related Federal laws, regulations, and policies.

SPECIFIC REQUIREMENTS ASSOCIATED WITH DATA BREACH ANALYSIS SERVICES INCLUDE:

a) Addresses all program areas as ordered
b) Initial report provided 30 calendar days after notification and quarterly thereafter
c) Review all information compromised by a data breach for trends and unusual patterns
d) Investigate the circumstances surrounding the breach to determine whether it appears to be incidental, accidental, or targeted
e) Analyze the breached data itself to determine if there is any current evidence of organized misuse
f) Provide reports to the Ordering Agency that include aggregate information about responses in order to allow the Ordering Agency the ability to quickly address questions from interested stakeholders
g) Conduct a review for evidence of compromise of protected information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing protected Contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been assessed as a result of the incident in order to identify compromised protected information, or that affect the Contractor's ability to perform the requirements of the contract

SPECIFIC REQUIREMENTS ASSOCIATED WITH DATA BREACH RESPONSE AND IDENTITY THEFT SERVICES INCLUDE:

The Contractor shall establish a dedicated, branded website for impacted individuals to enroll themselves and access all data breach recovery services. The Government may require the site to link with a .gov web page and must meet the following performance standards:

a) Must be 508-compliant
b) Must be IAW NIST SP 800-53 (latest revision) but have the capabilities to meet NIST SP 800-171 (latest revision) if required at the Task Order level. Website shall be accessible on major commercial browsers (i.e. Internet Explorer, Chrome, Firefox, Safari, and Opera) as well as mobile optimized to render to mobile screen resolutions on major commercial mobile browsers (i.e. Safari and Chrome)
c) Fully operational in advance of notification to impacted individuals
d) 99.00% operational
e) Must support the use of a single use activation (PIN) code that is unique for each impacted individual.
f) Multifactor authentication for impacted individuals utilizing known and unknown factors to the affected individual such as Data at Rest Encryption; Data in Transit Encryption; Data Loss Prevention; Database HIDS; etc.

SPECIFIC REQUIREMENTS ASSOCIATED WITH A CALL CENTER INCLUDE:

The Contractor shall establish call center services with service specialists capable of assisting individuals and the call center shall meet the following performance standards:

a) Operational prior to notification of impacted individuals
b) Located in the U.S.
c) English and Spanish, or as otherwise indicated at the Task Order level
d) Dedicated U.S. toll-free telephone number
e) 508-compliant and free international telephone access (international TTY applicability to be determined by ordering agency)
f) Automated Interactive Voice Response (IVR) and call enter tool for eligibility and activation (PIN) code lookup based on an individual providing full or truncated fields of personally identifiable information on which to be matched
g) Use call center FAQs provided by the Federal Government
h) Updated FAQs shall be used upon receipt

The Contractor shall respond to queries, enrollments, and requests for use of provided services from impacted individuals and shall meet the following performance standards:

a) Wait times not to exceed 15 minutes before human assistance is rendered
b) Average wait time shall not exceed 10 minutes
c) Maintain daily call log
d) Call center hours 24 hours a day, 7 days a week
e) Provide call logs for review by Ordering Agency Contracting Officer or assigned designee (including number of calls, wait time, length, dropped calls)

The call center services shall include:

a) Operational Status of the call center established for impacted individuals under the Task Order summarized in percentages (reporting period and cumulative)
b) Number of calls received (reporting period identified in order and cumulative)

c) Number of calls abandoned (reporting period identified in order and cumulative)
d) Number of enrollments by call center (reporting period identified in order and cumulative)
e) Summary of performance against standards established for call center including remedy and plans to prevent future occurrence if standard is not met (reporting period only)

The Contractor shall connect impacted individuals to designated identity restoration services and identity theft insurance services and which include meeting the following standards:

a) Ongoing basis
b) Initiation of the process for use of the Identity Restoration Service or Identity Theft Insurance within 15 minutes of impacted individual making contact with a live person at the call center.

The Contractor shall forward and present special requests or issues collected on a daily basis from impacted individuals to the Government for further consideration. Special requests or issues include those requests or issues from impacted individuals who have not been provided the necessary level of information from the Contractor. This list shall also include repeated questions from impacted individuals that are not covered in the FAQs.

SPECIFIC REQUIREMENTS ASSOCIATED WITH NOTIFICATION INCLUDE:

a) Delivery status of all Task Order Government Furnished Information
b) Status of data cleanse with estimated completion date
c) Status of deduplication of data with estimated/actual completion date
d) Estimated number of impacted individuals
e) Total number of notifications planned to be sent via USPS First Class mail
f) Total number of notifications mailed via USPS First Class Mail by Contractor
g) Total number of returned mail notifications
h) Total number of redistributed mail notifications after being returned

The Contractor shall intake, review, and data cleanse the PII and/or PHI Government furnished data set. This will include review of national change of address (NCOA).

The Contractor shall deduplicate the data cleansed list and provide duplicative data list and final notification list for approval by the Government. Deduplication of data is the removal of repetitive information for the same individual. The Contractor will be required to meet the following performance standards:

a) Ensure 99% of records are accurate
b) Ensure that the deduplication services are completed within seven (7) business days.
c) Will use the following format: XML or CSV
d) Provide both a duplicate and final list of data cleansed
e) Support the use of a unique id per record to reduce and/or remove the exchange of PII required in the provided result data

The Contractor shall review Government furnished language and make recommendations to the Government. Government furnished language includes but is not limited to letters, emails, and FAQs. The Contractor's review shall provide recommendations in the same format provided by the Government within three (3) business day.

The Contractor shall prepare Government approved content and formatted mail notifications for all impacted individuals upon approval of the Final List by the Government. The notification shall contain a unique *.gov* website link provided by the Government and the Contractor must have the ability to maintain or regenerate a copy of the notification distributed to impacted individuals. The *.gov* website will contain a direct link to the Contractor's website established for the services required.

The Contractor shall distribute notifications to impacted individuals within five (5) calendar days (unless otherwise stated at the Task Order level) upon receiving the approved Final LIst by the government . The Contractor shall distribute notification by zip code. The Contractor shall establish a unique PO Box return address for distributed mail. The return address shall contain an OPM identifier.

The Contractor shall provide a list of failed notifications to the Government within no less than fourteen (14) calendar days (unless otherwise stated at the Task Order level) after all notifications have been sent. This process must remain in effect in an ongoing basis.

The Contractor shall redistribute previously failed notifications to impacted individuals within five (5) calendar days (unless otherwise stated at the Task Order level), after receiving additional identifying information from the Government.

The Contractor shall respond to queries, enrollments, and requests for use of provided services from impacted individuals. The Contractor shall authenticate the identity of impacted individuals who desire to enroll using the data provided by the Government. Once authenticated, any impacted individuals may enroll themselves. Impacted individuals who opt to use the call center may be able to authenticate their eligibility via touch tone phone prior to advancing to a call center attendant. The Contractor shall have an automated recording protocol that accommodates all callers, including addressing instances where individuals are not eligible for the services.

SPECIFIC REQUIREMENTS ASSOCIATED WITH CREDIT MONITORING SERVICES INCLUDE:

Upon enrollment, the Contractor shall provide, at a minimum, credit monitoring of credit reports from Experian, Equifax, and TransUnion, however, an Ordering Agency may request inclusion of other Credit Reporting Agencies at the Task Order level. The Contractor will be required to meet the following performance standards:

a) Initial credit report for impacted individuals to be available within 48 hours of enrollment into credit monitoring services
b) Identify all changes in credit reports
c) Identify and notify impacted individuals of any additional findings or changes no

later than 24 hours after occurrence
d) Provide all three bureau reports annually in accordance with the Fair Credit Reporting Act
e) Be in accordance with Federal and applicable State Laws

A summary of all credit monitoring services will be provided (report period and cumulative) and will include:

a) Number of impacted individuals who enrolled in services
b) Number of impacted individuals enrolled
c) Number of individuals to whom credit reports from all three national credit reporting agencies have been made available
d) Number of individuals that were notified of changes to their credit file
e) Number of individuals who opened identity restoration cases

SPECIFIC REQUIREMENTS ASSOCIATED WITH IDENTITY MONITORING INCLUDE:

The Contractor shall provide identity monitoring services for enrolled individuals. Identity monitoring services includes, but is not limited to:

a) Monitoring of the Internet and the dark web for personal information including but not limited to, social security number, phone number(s), email address(es), credit and debit card number(s), medical identification number(s), driving license, and passport number
b) Monitoring of database sources including, but not limited to, criminal records, arrest records, court records, change of address, and social security number trace which notifies an individual of names and addresses associated with their social security number
c) Monitoring will be 24 hours a day, 7 days a week
d) Contractor will identify and notify impacted individuals of findings or changes no later than 24 hours after Contractor's monitoring discovers occurrence

A summary of all identity monitoring services will be provided (report period and cumulative) and will include:

a) Number of impacted individuals enrolled
b) Number of individuals that were notified of potential suspicious activity. (The Contractor will be required to provide the location of suspicious activity (i.e., Internet or specific monitored database))
c) Number of individuals that confirmed activity was suspicious (The Contractor will be required to provide the location of suspicious activity (i.e., Internet or specific monitored database))

SPECIFIC REQUIREMENTS ASSOCIATED WITH IDENTITY THEFT INSURANCE INCLUDE:

The Contractor shall provide identity theft insurance to impacted individuals regardless of their enrollment status in other services. The insurance shall cover any fraudulent misuse of an impacted individual's PII and/or PHI. Coverage will include all claims submitted on or prior to:

(as defined in the Task Order). The terms of the insurance agreement agreed to at time of GSA Schedule award shall include up to $5,000,000.00 per impacted individual, with no deductible. The benefits of this insurance shall include, at a minimum, coverage of:

a) Lost wages
b) Travel expenses
c) Elder care and child care
d) Legal costs for attorney fees for defense of any legal action brought against a subscriber for identity theft related items
e) Any other expenses specifically tied to identity restoration
f) Unauthorized electronic fund transfer reimbursement

A summary of all identity theft insurance will include:

a) Number of individuals requesting identity theft insurance services
b) Status of claims submitted to include the number of open claims
c) Number of closed claims, total value of insurance claims submitted by impacted individuals, total value of insurance expenses paid to impacted individuals (both open/closed claims), total amount of insurance payments to individuals with closed claims, types of claims submitted (e.g., lost wages, travel expenses), and a description of services rendered

SPECIFIC REQUIREMENTS ASSOCIATED WITH IDENTITY RESTORATION SERVICES INCLUDE:

Identity restoration services will include, but are not limited, to the number of impacted individuals requesting identity restoration services.

The Contractor shall provide identity restoration services for all impacted individuals regardless of their enrollment status in other services. The scope of this coverage includes any identity theft claim submitted within the period of performance of the Task Order to restore the identity to the pre-compromised state.

The Contractor shall assign an individual case manager to work with the impacted individual requiring identity restoration services to restore the identity to the pre-compromised state.

The Contractor shall offer the option of working under the authority of a Limited Power of Attorney, when required. These services shall include, but not be limited to, counseling, investigation, and resolving identity theft issues and the following performance standards must be met:

a) Ongoing basis
b) Assign a case manager who will contact the impacted individual within the time specified at the Task Order level
c) Case managers are Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transactions Act (FACTA) certified

The Contractor will provide a status of claims submitted to include:

a) Number of open identity restoration cases

b) Number of closed identity restoration cases
c) Type and quantity of services rendered to restore identity
d) A description of the services rendered

SPECIFIC REQUIREMENTS ASSOCIATED WITH REQUIRED REPORTS INCLUDE:

The Contractor shall provide reporting as defined in the Task Order. An example reporting requirement is provided as follows: The Contractor shall provide a Status Report to accurately reflect the status of its website services, to include:

a) Operational Status of the website established for impacted individuals under the Task Order summarized in minutes (reporting period identified in order and cumulative);
b) Number of times accessed (reporting period identified in order and cumulative);
c) Number of enrollments in services by website (reporting period identified in order and cumulative);
d) Description of any events related to interoperability of website including remedy and plans to prevent future occurrence (reporting period only);
e) Customer feedback provided through website (reporting period only)

The Contractor generated format for any report provided at the Task Order level is subject to approval and feedback of Government and must be in either .XML or CSV format. All reports provided to the Government shall clearly state the period start and end date/time of data.

SPECIFIC REQUIREMENTS ASSOCIATED WITH DATA SAFEGUARDS AND DISPOSAL SAFETY INCLUDE:

The Contractor shall:

a) Store and protect all data collected for the affected individuals during the designated time frame from unauthorized disclosure and destruction, either direct or as a result of negligence.
b) Purge all PII/PHI data (data sanitization) provided by the Ordering Agency in accordance with DoD 5220-22-M, National Industrial Security Program Operating Manual, and NIST SP-800-88 (latest revision), including any backed-up data and any other PII or PHI held by the Contractor pursuant to this agreement and safely dispose as agreed to by the Ordering Agency at the conclusion of the last enrollee's period of monitoring.
c) Within 30 calendar days after the end of the performance period, the Contractor shall provide notification to the Contracting Officer. The notification shall include a description of the information that will be destroyed, as well as, a description of the information required for completion of pending/ongoing restoration claims. The Contractor shall not destroy any information without written approval from the Contracting Officer. The Contractor shall certify to the destruction of all protected information no more than 30 calendar days after receiving written approval from the Contracting Officer, with the exception of information needed for pending and ongoing restoration claims.

The Contractor shall certify in writing the date information was deleted and method used for deletion.

d) All PII or PHI will be maintained, handled, disclosed, and disposed of in accordance with the Privacy Act of 1974, 5 U.S.C. 552a, Public Law 107-347 titled E-Government Act of 2002, the Federal Records Act, and the Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009.
e) The Contractor shall guarantee strict confidentiality of the information/data that is provided by the Government during the performance of any Task Order.
f) The Contractor, in whole or in part, can only disclose or disseminate the information/data, after they have received written approval from the Ordering Agency Contracting Officer.
g) Contractor personnel assigned to the performance work are required to certify that all employees hired for the resultant task have employment background checks in compliance with the Fair Credit Reporting Act (FCRA) 15 U.S.C. § 1681 dated September 2012. If at any time during performance of any Task Orders awarded against this GSA Schedule contract, the Contractor personnel are deemed a security risk, the Contractor will be responsible for immediate removal from performance under the Task Order and replacement of acceptable personnel with notification immediately provided to the Ordering Agency. Upon removal or completion, Contractor personnel shall immediately return any facility access materials/passes to the Ordering Agency Contracting Officer.
h) The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information.
i) The Contractor, employee of the Contractor, Contractor subcontractor, or partner to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed or disseminated only for a purpose and to the extent authorized herein. Any request for inter-agency sharing of information about individuals shall comply with OMB Memorandum M-01-05, “Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy.” The Contractor shall keep the information confidential and use appropriate safeguards to maintain its security in accordance with minimum Federal standards.
j) The Contractor must also explain and certify that its subcontractor(s) or partners will adhere to the same minimum Federal standards when working with sensitive data.
k) The Contractor shall not use the information for any purpose other than contacting the affected individual. Any type of marketing, up-selling, after marketing, or soliciting of any individuals is prohibited. Services provided shall be performed in accordance with applicable Federal laws and policies including the Identity Theft and Assumption Deterrence Act, as amended by Public Law 105-318, 112 Statute 3007 (Oct. 30, 1998), and implemented by 18 U.S.C. § 1028.
l) The Contractor is required to adhere to Federal Information Security Modernization Act (FISMA) of 2014 and all applicable OMB policies, including any policies issued during the term of its Schedule contract. This includes any

updates to OMB Memorandum M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information”.

m) The Contractor will provide recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

n) The Contractor must cooperate with the designated Ordering Agency or other designated Government Agency inquiries into the suspected loss or compromise of PII and PHI. This includes meeting the designated Agency's data breach incident reporting requirements.

At the Government’s discretion, the Contractor’s employees (or affiliated partners or subcontractors) may be identified as no longer eligible to access PII and PHI or to work on that contract based on their actions related to the loss or compromise of PII and PHI.

The Government has determined that the information/data that the Contractor will be provided during the performance of any effort associated with SIN 520-20 is of a sensitive nature and the Contractor is explicitly required to notify the agency of any subpoena, court order or other third party request for the Government’s records (e.g., any individual email addresses or other nonpublic information that may have been given to or generated by the Contractor in performing work under any Task Order). Failure to comply with this requirement may result in legal and or criminal infraction.

Whenever the Contractor is uncertain with regard to the proper handling of information/data under any effort associated with SIN 520-20, the Contractor shall obtain a written determination from the Ordering Agency Contracting Officer.

TASK ORDER AWARD REPORTING REQUIREMENTS:

The Contractor shall provide email notification within five (5) days of all new task orders awarded. The notification shall include a brief description of the task, name of the requiring entity, period of performance, and estimated dollar value. In addition, the notification shall include one complete copy of each order, including the statement of work. Notification shall be submitted to IPS_PSS@gsa.gov.

SECTION II - ADDITIONAL SERVICES

Additional services are customized solutions needed that can only be ordered in *addition* to IPS Requirements Document 1A Section I services. These additional services may utilize the services found under SINs 520-16, Business Information Services, and 520-17, Risk Assessment and Mitigation Services. Section II additional services **shall not** be ordered as a stand-alone service for Task Orders under SIN 520-20.

Identity Protection Services (IPS)
IPS Document 1B
in Support of SIN 520-20

ADDITIONAL PROPOSAL INSTRUCTIONS

Reference IPS Requirements Document 1A In addition to the standard solicitation proposal requirements, Contractors will be required to meet the following requirements with their GSA Schedule contract submittal (or modification to add SIN 520-20) that include:

SECTION I - TECHNICAL PROPOSAL

A narrative detailing the following:

- Firm's general management approach to providing each of the required services described in IPS Requirements Document 1A, Section I.

- Demonstration of how firm will provide services required, including compliance with all required standards throughout the period of performance.

- A detailed System Security Plan will be submitted in accordance with NIST SP 800-53 (latest revision) using the attached template. The firm's responses will be required to be complete and clear with each element addressed. Failure to follow the plan or complete any segment of the plan will result in rejection of a firm's offer. It is noted that if a specific plan is not requested at the Task Order level, the firm will be required to utilize the same template awarded at the GSA contract level.

  NOTE 1: In addition to the required System Security Plan, ancillary documents may also be required by the Ordering Agency which will be validated at the Task Order level.

  NOTE 2: Plans that do not follow the attached guidance will be rejected as unacceptable. Plans that simply parrot back the security requirements of NIST SP 800-53 (latest revision) are not acceptable and will result in rejection of offer.

  NOTE 3: If any changes/updates are required to the approved Systems Security Plan at the Task Order level, the Contractor will be required to submit an updated plan to the Ordering Agency and provide a copy of that revised plan to the GSA IPS Program Manager upon approval by the Ordering Agency for review and incorporation.

Identity Protection Services (IPS)
IPS Requirements Document 1B (continued)
in Support of SIN 520-20

SECTION II - TECHNICAL PROPOSAL FOR ADDITIONAL SERVICES

Firms shall indicate in their proposal whether or not they are proposing to provide services under IPS Pricing Document 2, Section II Additional Services. There are no additional technical proposal requirements to be considered for these additional services. Follow the standard solicitation proposal requirements. In order to provide services under SIN 520-20 Section II Additional Services, a firm must qualify and be awarded SIN 520-16 or 520-17 in its Schedule contract.

System Security Plan (SSP):

Firms will be required to submit a System Security Plan (template identified as Identity Protection Services (IPS) IPS Requirements Document 1C in Support of SIN 520-20), included in the solicitation.

All Contractors must complete this System Security Plan to be considered for SIN 520-20.

Identity Protection Services (IPS)
IPS Pricing Document 2
in Support of SIN 520-20

SECTION I - PRICING:

NOTE: Ordering agencies have the flexibility to order some or all of the services as defined in SIN 520-20, however, a System Security Plan must be provided for any or all services offered.

In order to be considered for award of SIN 520-20, the Contractor is required to provide pricing for a total solution covering ALL the services described in Section I of IPS Requirements Document 1A in support of SIN 520-20.

Prices offered must be "Price Per Month/Per Impacted Individual" at the Schedule contract level. Ordering Agencies maintain the flexibility to utilize this fixed pricing as a basis to further quote fixed prices at the Task Order level (e.g. "per product redeemed per the agreed-upon coverage period (month, year, etc.)").

Number of Impacted Individuals	Firm Fixed Price Per Month/Per Individual
1-100	$
Over 100 to 1K	$
Over 1K to 5K	$
Over 5K to 25K	$
Over 25K to 50K	$
Over 50K to 250K	$
Over 250K to 1M	$
Over 1M to 10M	$
Over 10M to 20M	$
Over 20M to 30M	$
Over 30M to 50M	$
Over 50M	$

Discount Description	Discount percent on Per Month/Per Individual Price
Dedicated Branded Website not required	%
Dedicated U.S. Toll-free number not required	%

24/7 Call Center hours not required	%
Only $1M Insurance required	%

Note: Above prices may be further discounted at the Task Order level.

In order to accommodate a requirement for only some of the services identified in Section I (e.g., credit monitoring only), firms offering SIN 520-20 are encouraged to provide individual line item pricing below.
*(**Firm is welcome to add additional tables as needed**):*

Pricing is offered for: (*Firm to cite separate service offered*)

Number of Impacted Individuals	Firm Fixed Price Per Month/Per Individual
1-100	$
Over 100 to 1K	$
Over 1K to 5K	$
Over 5K to 25K	$
Over 25K to 50K	$
Over 50K to 250K	$
Over 250K to 1M	$
Over 1M to 10M	$
Over 10M to 20M	$
Over 20M to 30M	$
Over 30M to 50M	$
Over 50M	$

Note: Above prices may be further discounted at the Task Order level

SECTION II - PRICING FOR ADDITIONAL SERVICES:

Additional services are customized solutions needed that can only be ordered in *addition* to IPS Requirements Document 1A Section I Firm Fixed Price services ordered. These additional services may utilize the services found under SINs 520-16, Business Information Services, and 520-17, Risk Assessment and Mitigation Services. Section II additional services **shall not** be ordered as a stand-alone service for Task Orders under SIN 520-20.

Pricing for these additional services shall utilize the labor categories/rates and/or items/prices

from SINs 520-16 and/or 520-17 of the Schedule contract as agreed to at the Task Order level accordingly.