Federal Trade Commission
First Amended Statement of Work for:

Consumer Information System
Consumer Response Center
National Do Not Call Registry

TABLE OF CONTENTS

CIS SOW Technical Exhibits

CIS TE 1	Consumer Sentinel Network User Application
CIS TE 2A	CIS Statspack Report
CIS TE 2B	CSDM Statspack Report
CIS TE 3	Online Identity Theft Complaint Report (future)
CIS TE 4	CIS and CSDM user account information
CIS TE 4A	VeriSign certificates
CIS TE 5	Non Disclosure Agreement
CIS TE 6	Office of Management and Budget Memorandum (OMB) M-06-16
CIS TE 7A	FTC Enterprise Database Security Policy
CIS TE 7B	FTC Sensitive Information Handling Policy
CIS TE 7C	FTC Enterprise Encryption Policy
CIS TE 7D	FTC Server Security Policy
CIS TE 7E	FTC Password Policy
CIS TE 7F	FTC IT Audit Policy
CIS TE 7G	FTC System Security Certification and Accreditation Policy
CIS TE 8A	Current general complaint web form
CIS TE 8B	Current Spanish-language general complaint web form
CIS TE 8C	Current Military Sentinel general complaint web form
CIS TE 8D	Current econsumer.gov complaint web form (English)
CIS TE 8E	Current IDT complaint web form
CIS TE 8F	Current Spanish-language IDT complaint web form
CIS TE 8G	Current Military Sentinel IDT complaint web form
CIS TE 9A	Records received by category (2003 – 2006)
CIS TE 9B	CIS Stats (2003 – 2006)
CIS TE 10A	Background on current crosswalks
CIS TE 10B	Georgia Governor's Office/NW3C Complaint Transfer Diagram
CIS TE 10C	Georgia Governor's Office/NW3C Complaint Transfer Narrative
CIS TE 11	2005 Requests for Assistance re CIS/Consumer Sentinel
CIS TE 12	CIS Architecture (Nov. 8, 2005)
CIS TE 13	IDT Architecture (Sept. 2005)
CIS TE 14	CIS user session information
CIS TE 15	FTC server architecture
CIS TE 16	IDT Data Dictionary
CIS TE 17	CIS Database Overview (including database tables)
CIS TE 18	CIS System Users
CIS TE 19	CIS Architecture Diagram (2)
CIS TE 20	DNC Architecture Diagram
CIS TE 21	CIS/IDT/DNC Complaint Data Flow
CIS TE 22	Consumer Sentinel GPRA stats (Sept. 2006)
CIS TE 23	Consumer Sentinel member agencies (2002 – 2006)
CIS TE 24	List of Consumer Sentinel Network Member Agencies (Oct. 10, 2006)
CIS TE 25A	IDT Associated Institution Data Flow
CIS TE 25B	IDT Credit Bureau Institution Data Flow
CIS TE 25C	Business Rules for CRA (IDT) Complaint Calls

Note: Parts C.1 through C.4 of the CIS Statement of Work (SOW) apply to the Consumer Response Center SOW and the Do Not Call SOW as well.

C.1 GENERAL INFORMATION

C.1.1 Introduction

This requirement is for performance-based technical services to build and operate a storehouse of consumer data relating to the Federal Trade Commission's (FTC) consumer protection mission. The contractor is required to perform the following specific tasks:

- Gathering, processing, updating and housing consumer information about instances of business practices related to fraud, financial loss, deceptive practices, identity theft, and National Do Not Call (DNC) Registry violations. This information may be collected directly by the FTC's call center and web based complaint forms, as well as indirectly through data imports from other organizations.

- Providing the FTC, as well as local, state, and federal and international law enforcement agencies, with access to the consumer information through queries and ad hoc reporting tools.

The contractor shall perform the following specific tasks pursuant to the corresponding Statement(s) of Work (SOW):

- Consumer Response Center (CRC) SOW: The contractor shall gather, process and update consumer information via call center services and web based complaint forms. The contractor also shall provide FTC consumer education materials to the public.

- National Do Not Call Registry (DNC) SOW: The contractor shall develop, implement and operate a national do not call registry that will permit United States consumers to register their preference not to receive telemarketing calls at the registered telephone numbers. The initial database build will be based on existing data in the registry. The specific tasks in the DNC (Option 2) SOW are divided into four main parts: consumer registration; telemarketer and seller access; law enforcement access; and consumer complaint processing.

C.1.2 Background[1]

C.1.2.1 Federal Trade Commission

The FTC is the primary federal agency with broad jurisdiction to enhance consumer welfare in virtually all sectors of the economy. The FTC enforces the laws that prohibit

[1] The information presented in the "Background" section, including descriptions of the manner in which the current data collection and analysis system works, is for factual and historical purposes only. Other than stated in the Specific Tasks section, the FTC is in no way requiring that the system to be developed and provided by the contractor shall operate in the same manner.

business practices that are anticompetitive, deceptive, and unfair to consumers. The agency also promotes informed consumer choice and public understanding of the competitive process. The FTC's work is critical in protecting and strengthening free and open markets in the United States and the global marketplace.

The FTC has two law enforcement bureaus, Consumer Protection and Competition, supported by the Bureau of Economics and regional and mission support offices.

C.1.2.2 Bureau of Consumer Protection

The Bureau of Consumer Protection (BCP) enforces a variety of consumer protection laws. Its law enforcement-related activities include consumer complaint collection and analysis, individual company and industry-wide investigations, administrative and federal court litigation, rulemaking proceedings, and consumer and business education. One consumer protection initiative by the FTC includes amendments to its Telemarketing Sales Rule (TSR). A core component of the TSR amendments required implementation of the National Do Not Call (DNC) Registry, which has significantly impacted the Bureau's law enforcement activities.

C.1.2.3 Consumer Information System

BCP uses the Consumer Information System (CIS) as the primary system to collect, analyze, extract, distribute, and archive/purge data relating to its mission. In addition to recording instances of business practices related to fraud, financial loss, identity theft, and DNC complaints, CIS also facilitates consumer requests for educational material. As of September 25, 2006, CIS contained approximately 6.07 million records.

As a central repository for this data, CIS is a powerful crime-fighting data source, much of which is available to the federal, state, and local, as well as international, law enforcement community. In addition, CIS data is used to identify and track trends and potential problems affecting the marketplace.

CIS interconnects several applications within the FTC. One of these applications, the Consumer Sentinel Network, currently serves more than 9,000 law enforcement users across the world. These applications, comprised of secure restricted websites which permit limited access to CIS, provide users with integrated access to the worldwide justice network of about 1,600 law enforcement agencies (for a list of current Consumer Sentinel Network member agencies, see CIS Technical Exhibit 24). Through this network, federal, state, local, and international law enforcement and justice agencies have access to a comprehensive set of consumer protection-related complaints.

The majority of the records in CIS are received by the FTC's Consumer Response Center (CRC) through two toll-free telephone numbers, online complaint forms, and mail. These records include consumer complaints and requests for information. Other public and private entities share consumer complaint data with the FTC, which is entered into CIS.

Currently, the CIS database is maintained at the FTC's Headquarters building. The sizes of the CIS and related Consumer Sentinel Data Mart (CSDM) are 47G and 60G, respectively, for data and index (actual used) content space. These figures do not include ancillary space needed to house the application. CIS and CSDM transaction times, sample searches, and related data are in CIS Technical Exhibit 2.

CIS currently stores complaints in English, Spanish, French, and German. All content is stored as it is entered - not translated to a common searchable text (i.e., English). Since foreign language content has been a very small percentage of the content currently stored in CIS, the FTC has not addressed the use of desktop language kits, client fonts or browser parameter recommendations.

C.1.2.4 Relevant CIS System Components or Ancillary Systems

C.1.2.4.1 Consumer Sentinel Data Mart

The Consumer Sentinel Data Mart (CSDM) was designed and developed to improve performance of the CIS applications. By separating ad-hoc and long-running queries from the CIS transaction database, the Data Mart is the query and reporting repository for the Consumer Sentinel Network (see description below). The CSDM also houses the DNC consumer complaints. The purpose of the CSDM is to store information in a manner optimized for reporting (output, queries) as opposed to transactions (input from CRC, Internet or data from external contributors). The contractor does NOT need to follow the example of using a separate data warehouse.

C.1.2.4.2 Online Complaint Forms

The FTC operates several public websites where consumers can lodge general consumer and identity theft complaints, obtain educational materials, and view trends in fraud and identity theft. General consumer and identity theft complaint forms are available in English and Spanish. The public websites through which the FTC collects online complaints that are entered into CIS are:

- The FTC's primary website at www.ftc.gov for general and identity theft complaints;
- The FTC's Spanish language website at www.ftc.gov/espanol for general and identity theft complaints in Spanish;
- The Consumer Sentinel public website (www.consumer.gov/sentinel) for consumer complaints;
- The IDT website (www.consumer.gov/idtheft) for identity theft complaints;
- The econsumer.gov website (www.econsumer.gov) for complaints relating to cross-border e-commerce fraud (which provides online complaint forms in English, Spanish, French, and German (the FTC also will provide Japanese and Polish translations and the contractor will create the complaint forms in these languages);

- The Military Sentinel public website (www.consumer.gov/military), for complaints from service members, their families, and DOD civilians. In addition to the standard information collected on the FTC's other online complaint forms, the complaint forms on Military Sentinel allow consumers to identify their service branch, status, posting and pay grade; and

- The Do Not Call website (www.donotcall.gov) for complaints related to violations of the TSR and the DNC Registry (as explained in more detail below, these complaints are collected by the DNC vendor and transferred to CIS).

C.1.2.4.3 Consumer Sentinel Network

The Consumer Sentinel Network (CSN) is a series of interconnected web based applications, or portals, through which external users (and internal FTC users) can access various subsets of complaint records in CIS. These applications include: Consumer Sentinel, the Identity Theft Data Clearinghouse, Consumer Planet Sentinel, and Military Sentinel. (In-depth descriptions of each are in the following sections.) External users have access only to the Consumer Sentinel Network and not directly into CIS.

C.1.2.4.3.1 Consumer Sentinel

The purpose of Consumer Sentinel (CS) is to collect and share information about consumer fraud, identity theft and DNC with law enforcement agencies. CS is accessible free of charge to local, state and federal law enforcement agencies ("members") in the United States, Canada and Australia. Individual users access CS through a secure, password-protected website. Depending on their privileges, they then can search millions of fraud, identity theft and DNC complaints. (This represents a subset of the records in CIS.) Search criteria includes, among other things, company or suspect name, address, telephone number, consumer location, or type of scam or identity theft.

In implementing a solution, the contractor should expect that CS users will be able to search through ALL non-identity theft (general) records, as opposed to only those complaints categorized as fraud.

In addition to searching for complaints, CS has a variety of tools to aid users. These tools include:

1. An "alert" function that allows users to flag companies, suspects and identity theft victims that are part of an investigation in order to inform other law enforcers using CS.

2. An "auto query" function that will periodically scan the database for new complaints relating to the user's interest and notify the user via email if it finds any new complaints meeting their criteria.

3. Top violators reports that allow users to identify companies or individuals receiving the most complaints.

4. Consumer fraud and identity theft trend reports prepared by FTC data analysts.

5. An index of taped, allegedly fraudulent telemarketing sales pitches available from the National Tape Library.

6. A list of all registered CS users with contact information.

7. Contact lists for regional and cross-border fraud and identity theft law enforcers.

8. A library of reference materials and website links, how-to manuals for investigating different types of fraud, and periodicals.

9. The ability to add complaints on behalf of consumer fraud and identity theft victims. These complaints are then entered into CIS.

C.1.2.4.3.2 Identity Theft Data Clearinghouse

The Identity Theft Data Clearinghouse is the nation's repository of identity theft complaints. Users access the Clearinghouse through CS. Accordingly, users conduct searches of the Clearinghouse in the same manner as on CS. As of September 25, 2006, there were about 1.19 million identity theft complaints accessible through the Clearinghouse.

Currently, the data in the Clearinghouse is available to all domestic law enforcement agencies that have signed an appropriate agreement with the FTC. Eligible Canadian law enforcement members may view a subset of the IDT complaints. No other foreign law enforcement agency may view the IDT complaints; however, this may change in the future.

As part of the President's Identity Theft Task Force Summary of Interim Recommendations (http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf), the FTC, with support from Task Force members, has developed a universal police report/identity theft complaint. Identity theft victims can complete the complaint online, print it, and take it to a local law enforcement agency for verification and incorporation into the police department's report system.

For the future, the FTC envisions that in law enforcement agencies that are Consumer Sentinel Network members, an officer will call up the complaint, stored in CIS. The officer will interview the victim to verify information. If the information in the report is verified, the officer will complete online the law enforcement authentication portion of the report (e.g., department name, local incident report number, etc.) and send it back to the database via the secure data transfer architecture. The officer then will print out a copy of the IDT report for the victim with law enforcement authentication information.

For law enforcement agencies that are NOT Consumer Sentinel Network members, the FTC is researching methods to facilitate this process by securely connecting to a law enforcement data transfer network(s).

C.1.2.4.3.3 Consumer Planet Sentinel (econsumer.gov)

The Consumer Sentinel Network also houses Consumer Planet Sentinel (CPS). CPS membership is open to government agencies in those countries that belong to the International Consumer Protection and Enforcement Network. CPS is part of econsumer.gov (www.econsumer.gov), an international project focusing on cross-border e-commerce fraud. Like the Consumer Sentinel public website, econsumer.gov offers cross-border consumer protection information and an online complaint form. All information on econsumer.gov, including the complaint form, is available in English, Spanish, French, and German (the FTC anticipates Japanese and Polish language versions as part of this contract, and possibly other languages as well).

Cross-border e-commerce complaints received from consumers through the econsumer.gov complaint form are entered into CIS. CPS members can access only the econsumer.gov complaints through a secure, password-protected website. The FTC desires to provide CPS users with the same functions available to CS users (e.g., alert, auto-query, etc.).

C.1.2.4.3.4 Military Sentinel

Military Sentinel, which was launched in September 2002, is a joint initiative of the FTC and the Department of Defense (DOD) to identify and target consumer protection issues for service members, their families and DOD civilians. Military Sentinel also provides a gateway to consumer education materials covering a wide range of consumer protection issues. Information from complaints entered through Military Sentinel helps target law enforcement actions and consumer education initiatives.

The complaint forms on Military Sentinel allow consumers to identify their service branch, status, posting and rank. General and identity theft complaints entered into Military Sentinel go directly into CIS, and are accessible by users through CS and the Identity Theft Data Clearinghouse. Also, fraud complaints submitted through Military Sentinel's public website are accessible by DOD consumer education staffers through a restricted, password-protected website (also called Military Sentinel), although consumers' personal identifying information (e.g., name, address, telephone number) is not displayed. The FTC desires to provide Military Sentinel users with the same functions available to CS users (e.g., alert, auto-query, etc.).

C.1.2.4.3.5 National Do Not Call Registry

In October 2003, the FTC implemented the DNC Registry. The registry is a central database of telephone numbers of consumers who choose not to receive telemarketing calls. Consumers are able to register either online or by telephone. The TSR requires that telemarketers search the registry every 31 days and delete (or "scrub") from their call lists phone numbers that are on the registry. Since inception, there are over 132 million telephone numbers have been registered.

Consumers who receive telemarketing calls after they have registered their telephone numbers are able to lodge complaints either online or by telephone. These complaints are

entered into CIS and accessible through CS. As of September 25, 2006, there are about 2.37 million DNC complaints in the Consumer Sentinel Data Mart (DNC complaints are loaded directly into the CSDM; they are not loaded into CIS.)

The FTC has contracted with AT&T Government Solutions, Inc. to implement and maintain the consumer and telemarketer registries, and to receive consumer complaints. AT&T transmits all consumer complaint information to the FTC for storage in CIS via XML utilizing a web services approach on two redundant private T-1's. However, the consumer and telemarketer registries remain housed in AT&T databases. Both are accessible by CS users through Consumer Sentinel.

C.1.2.4.3.6 Crosswalks

In FTC parlance, a "crosswalk" provides mechanisms to upload bulk complaints into CIS (also called imports), request bulk downloads of complaints (also called exports), and administer the quality assurance (QA), scheduling, logging, and notification aspects of the process.

CIS currently receives batch data content from various other government and private entities. Data format is determined in agreement with the contributing organization. The FTC does not mandate a specific data format. The FTC maps the external format to CIS attributes. The external source may or may not provide all of the CIS attributes, and several of the contributor's internal codes must be translated to matching CIS internal codes.

For general complaints, the FTC utilizes the crosswalk service (an application built on J2EE and WebServices). The crosswalk service provides a means to QA the data before it goes into the database. XML is used throughout to describe the complaint data and the system data, such as logs, preferences, etc. The crosswalk service also facilitates bulk exports of general complaints for the credit reporting agencies. Other bulk general complaint exports require ITM support using SQL queries.

For import of identity theft complaints, the FTC uses a random structure of batch processes and desktop initiation from ITM administrators. Export of identity theft complaints requires ITM support using SQL queries.

C.1.2.4.4 CIS Users

C.1.2.4.4.1 FTC Users

Within the FTC, there are about 600 CIS user accounts. This number includes personnel who work for the CRC external call center vendor (see below for description). The total figure does not include the Office of Information and Technology Management (ITM) staffers responsible for maintaining the software applications and databases. The groups that comprise the FTC users include:

- **Consumer Response Center (CRC):** The CRC information specialists use CIS for the following purposes: enter and update fraud, identity theft and all other consumer

complaints received by phone, mail and online; respond to requests for information (on consumer fraud and identity theft, other areas of law within the FTC's jurisdiction, and brochures); enter and process inquiries from law enforcement and businesses; and enter general comments. When required, the contact center vendor sends a response to a consumer's complaint that includes a letter or a letter and educational brochures. These responses are currently fulfilled by the vendor from a remote location separate from the contact center.

The bulk of the complaints relating to unfair, deceptive, or fraudulent business practices are received from telephone contacts through the Commission's general consumer help line (1-877-FTC-HELP), which is currently operated by a contractor, Lockheed Martin Aspen Systems, Inc. This help line is configured to allow calls from within the United States, Canada, Puerto Rico, U.S. Virgin Islands, and other territories. Similar complaints are received via postal mail and Internet submissions from FTC operated websites (See: www.consumer.gov/sentinel; www.ftc.gov). The contractor information specialists enter the information provided by the consumers into CIS through a connection with the FTC's designated database manager. The information specialists also may respond to these contacts by preparing acknowledgment letters using pre-approved responses. Currently, there are approximately 17,000 weekly contacts for FTC-HELP via all channels.

The FTC also collects information about consumer complaints relating to identity theft. Information regarding this comes primarily from a dedicated telephone number (1-877-IDTHEFT), which was established when Congress passed the Identity Theft and Assumption Deterrence Act (ID Theft Act) in October 1998. This legislation requires the FTC to maintain a log of complaints received from identity theft victims, provide the victims with assistance and educational materials, and refer the complaints, in appropriate cases, to law enforcement authorities. BCP receives additional IDT data from written materials submitted by postal mail or through Internet submissions from FTC operated websites. The IDT data is entered into CIS. IDT volume currently is approximately 19,000 contacts via phone, online complaint forms, and mail per week.

Additionally, the FTC receives numerous complaints or inquiries concerning matters that are not within the jurisdiction of the FTC. Such requests are classified as "out - of-scope contacts." The contact center is required to record these contacts and refer them to the appropriate agencies for response.

In addition to the services provided by the contractor, the FTC also operates an internal Consumer Response Center (CRC), currently staffed by approximately 15 FTC employees. The CRC manages, processes, and redirects to the call center, the mail complaints that are then entered into CIS. Mail requests for brochures are handled by the CRC. Staff also reviews CIS and IDT electronic complaints before they are processed by the call center. The CRC also responds to questions received on the Commission's local business phone line, provides publications, brochures, and other written information to consumers and businesses, processes investigative

matters, supports law enforcement efforts, and provides assistance to phone counselors as needed. The FTC intends to continue to process at least a portion of the Internet communications received. The balance of these contacts may be referred to the contact center vendor for processing.

The FTC's in-house CRC staff performs quality assurance on the information entered into CIS by the contact center vendor. Also, in-house CRC staff preview online complaints and remove duplicates prior to processing by the contact center vendor. CRC staff also assist in cleaning up the database. In addition, FTC investigators in the in-house CRC use both CIS and CS to analyze complaint trends to identify companies requiring further investigation. Using other resources, the investigators develop preliminary investigative reports regarding consumer fraud scams. These leads are then sent to BCP law enforcement divisions and the FTC's regional offices.

Occasionally, employees at the CRC are asked to answer consumer calls on a temporary basis for some special purpose. Some of these special purposes range from active participation in certain law enforcement actions, active marketing of a toll-free telephone number or receipt of telephone calls about a specific topic. When situations warrant, the FTC may request the contact center contractor to reroute calls from the contractor operated center to the CRC for response. The anticipated volume and duration of such rerouting will be specified by FTC. CRC staff will need to be able to have calls escalated to them from the contact center or transfer calls to the call center as needed. The contact center must have the capacity to send and receive calls to and from CRC staff.

The offsite Lockheed Martin contact center accesses the database over a frame relay. Form files are stored at the call center to minimize calls to the database. Further, new records requiring a written response or brochure are duplicated in a CIS table which is shared with the call center, over the frame relay, and imported by the call center into their database for order fulfillment. The vendor also provides FTC staff access to a real time and call review application for QA purposes. This application allows the reviewer to view and listen to calls as they are being taken or that have been recorded recently.

- **FTC Consumer Protection Law Enforcement Staff:** The BCP and the FTC's regional offices are responsible for investigating and litigating cases involving fraudulent, deceptive and unfair practices. These investigators, paralegals, and attorneys conduct searches in CIS to identify targets and gather additional complaint information about suspects. CIS assists staffers in locating fraud victims, and they may use actual complaints or complaint counts to support litigation. BCP and the regional offices also use the alert and auto query tools, reports, telemarketing tapes and library. Occasionally, these staffers use CS to enter complaints on behalf of consumers.

- **FTC Office of General Counsel:** The Office of General Counsel responds to Freedom of Information Act (FOIA) requests. FOIA requests require searches on

CIS for complaints. If responsive complaints exist, all consumer personal identifying information must be redacted before the complaints can be released to the requestor.

- **BCP Data analysts**: The data analysts are responsible for analyzing information captured in fraud, identity theft and other (e.g., privacy-related) complaints in CIS, synthesize the information to identify trends and target suspect entities and individuals, and validate the results. The reports are prepared for the FTC, other law enforcement agencies, the media, members of Congress, and the public.

  As an example, each year the data analysts compile statistical data for the Consumer Fraud and Identity Theft Complaint Report (http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf), which is one of the FTC's most comprehensive studies. The report represents detailed analyses of the various categories of information captured in consumer complaints, and the graphic display of these analyses.

  In producing the reports, the data analysts use Business Objects to analyze the data in CIS (other BCP and regional office users also have access to, and use, Business Objects to report on CIS data). They validate the results using the Oracle search engine in CIS. The data is presented in various formats (e.g., PowerPoint, Business Objects reports, Excel, pdf files, Word and WordPerfect files) using graphics, charts and/or text.

  The analysts also assist in transferring crosswalk data received from external contributors into CIS. In addition, the analysts assist in clean-up of data stored in CIS, including eliminating duplicate records. They also help develop canned and ad hoc reports available to users on the Consumer Sentinel Network.

- **FTC Consumer Sentinel Team**: The Sentinel team currently is responsible for issuing CS Network user names and passwords. Also, they perform customer service for users, including training users to do searches and use system tools, troubleshooting access and systemic problems, conducting searches on behalf of users, and administering the content of the websites. The CS team participates in development of new features and functions on the CS Network. In managing the CS Network, the team works closely with both the software development and operational branches of ITM.

C.1.2.4.4.2 External Users

Through the CS Network, external users search on subsets of records in CIS. Access to the CS Network is restricted to local, state and federal domestic and foreign civil and criminal law enforcement agencies. Each agency (in the case of certain agencies, it may be a unit within it (e.g., fraud unit, inspector general) must sign a Consumer Sentinel Network Confidentiality Agreement. The Confidentiality Agreement is an agency-to-agency agreement. The agreement defines the CS Network access privileges and confidentiality rules.

Each individual CS Network user completes a one page application for access to the CS Network secure website. The information on the application is used to create an account for each individual Sentinel user. Each user receives a unique user ID and password.

In addition, each user must register for a VeriSign digital PKI certificate. The CS team reviews and approves the requests for certificates. Once issued, the certificate aids in authenticating the user for access to the secure CS Network website.[2]

- **Consumer Sentinel Members:** As of October 2006, CS had about 1,600 local, state and federal domestic, Canadian and Australian law enforcement member agencies. Law enforcers use CS search functions, alert and auto query tools, top violator lists and trend reports to identify fraud patterns and target suspect companies and individuals. CS users also enter complaints into CIS through the forms available on CS and the Clearinghouse. Most CS users have access to identity theft complaints. Certain domestic, Canadian and all Australian agencies do not have access to identity theft complaints. Currently, CS users are limited to searching for "fraud" complaints. It is anticipated that when the contractor's system is deployed, CS users will be able to search ALL CIS (non-identity theft) records.

- **Military Sentinel Members:** DOD non-law enforcement users mine complaints received through Military Sentinel to spot consumer fraud trends. They are then able to direct consumer protection materials to the correct service branch(es), installation(s) and personnel (by rank) based on the identified trends.

- **econsumer.gov/Consumer Planet Sentinel (CPS) Members:** These foreign government agencies use CPS in the same manner as CS users. They also add complaints to CIS through CPS. Currently, there are twenty-three (23) CPS member agencies.

- **External Data Contributors:** In addition to data entered into CIS by the CRC, the FTC receives complaint data from a broad array of public and private domestic and foreign organizations. Since 1997, users from about 40 CS Network members (including local, state, federal and international agencies) entered complaint data directly into CIS through their respective web applications.

  As previously discussed in the crosswalk section, other data contributors, including both CS members and non-CS entities, send complaints in other formats to be uploaded into CIS. The contributors' data transfers range from one complaint at a time up to tens of thousands of complaints. DPI maps data fields using contributors' data dictionaries.

[2] The VeriSign digital certificates have created a host of problems for CSN users due to the interaction between the certificates and member agency firewalls and network administration, as well as individual users' operating systems, web browser versions and web browser settings. The majority of CSN user customer support is dedicated to resolving certificate issues. The FTC is seeking alternatives to using these certificates commensurate with the sensitivity of the data and its security requirements.

- **External Data Receivers:** A very small number of domestic Sentinel members and the credit reporting agencies receive periodic batched downloads of complaints. This information is transmitted via CD. The largest individual batches to date have been about 350,000 complaints. These members either add the data to their own databases or, in the case of the U.S. Secret Service, use analytical software to identify patterns and report the results to the FTC.

C.1.3 Scope of Work

Except as specified in Section C.3 as government furnished property and services, the contractor shall provide all facilities, personnel, equipment, tools, materials, supervision and other items and services necessary to develop, implement and operate a system to store, analyze, extract, distribute, and archive/purge data relating to the FTC's consumer protection mission as defined in this SOW.

Under the CRC SOW, except as specified in Section C.3 as government furnished property and services, the contractor shall provide all facilities, personnel, equipment, tools, materials, supervision and other items and services necessary to develop and implement a system to collect data relating to the FTC's consumer protection mission and to establish a contractor-provided multi-channel contact center to support the operation of the programs described in this SOW.

Under the DNC SOW, except as specified in Section C.3 as government furnished property and services, the contractor shall provide all facilities, personnel, equipment, tools, materials, supervision and other items and services necessary to develop, implement and operate a national do not call registry as defined in this SOW.

The contractor must perform to the standards set forth in this contract. The estimated quantities of work are listed in the Technical Exhibits.

C.1.3.1 Work Volume Impact

Actual work volumes may be greater than or less than the volumes incurred to date. The FTC will notify the contractor of any known, or anticipated, impact to work volumes. The FTC anticipates that the following events may have an impact on work volumes:

a. The volume of telephone and email inquiries may increase as the FTC further promotes the help line and identity theft programs. The extent of the impact, however, is unknown at this time.

b. The FTC sponsors and/or participates in certain campaigns to promote consumer awareness (e.g., National Consumer Protection Week). These campaigns may cause a surge in call volumes. The extent of the impact on the work volumes will vary with the nature and scope of the promotional campaigns.

c. The FTC partners with law enforcement agencies, performing tasks that serve agency-specific programs on an as-needed basis (e.g., emergency response Hotline for Department of State).

On special operations involving certain law enforcement actions, active marketing of a toll-free telephone number, or receipt of telephone calls about a specific topic, the FTC may reroute calls destined for the contractor operated center to the FTC CRC for response. The reroute of such calls will reduce the call volumes to the contractor provided contact center for the duration of the special operations. The extent of the volume reduction will vary with the nature and scope and duration of the special operations.

C.1.4 Period of Performance

The period of performance of this SOW shall cover a transition and development period, a base performance period of one year, followed by four optional performance periods.

C.1.5 Transition and Start Up

For any of the SOW's awarded to the contractor, the contractor shall not start work on these tasks until it receives written notification to do so from the contracting officer ("the notification date"). For all of the SOW's, the FTC anticipates no more than 90 days for full transition. During this period, the contractor shall work with the FTC to develop a sound project implementation plan. The contactor shall work with the FTC and, if applicable, the incumbent contractor(s) to facilitate a smooth and seamless transfer.

CIS SOW: The contractor shall develop and implement CIS by no later than April 1, 2008.

CRC SOW: The FTC expects the contractor to begin transition of call handling with an appropriate staffing plan at least 15 days prior to assuming full work. The current contact center contract expires on March 31, 2008.

DNC SOW: The contractor shall develop and implement all components of the SOW by no later than October 1, 2007. The current DNC contract expires September 30, 2007.

C.1.6 Contractor Personnel

C.1.6.1 Contract Manager

The contractor shall provide a contract manager who shall be responsible for the performance of the work. The name of this person, and an alternate or alternates who shall act for the contractor when the contract manager is absent, shall be designated in writing to the contracting officer. The FTC reserves the right to approve the contract manager. If the FTC determines that the contract manager is unacceptable, the contractor shall replace the contract manager within 30 days. The contract manager or alternate(s) shall have full authority to act for the contractor on all contract matters relating to the daily operation of this contract.

The contract manager or alternate(s) shall be available Monday through Friday, except federal holidays, between 9:00 am and 8:00 pm Eastern time, within one hour of notification to meet or talk with FTC personnel designated by the Contracting Officer's Technical Representative (COTR). Outside of those days and hours, the contract manager or alternate(s) shall be available within four hours.

In the event the contract manager departs, the contractor shall provide immediate and complete mission and functional coverage until a replacement is available. A replacement is required within 30 days after departure of the contract manager. The contractor shall provide the FTC with the resume of the replacement. The contractor shall obtain the FTC's approval of the replacement contract manager.

C.1.6.2 Key Personnel

In addition to the contract manager, the contractor shall designate key personnel. Key personnel are contractor employees with authority to act, make decisions, and commit contractor resources to accomplish the workload or resolve issues during normal and emergency situations. At least one member of the key personnel will be on-site at the FTC Headquarters building one to two business days each week. The contractor shall provide the contracting officer with a list of key personnel and alternate or back-up designations. The FTC reserves the right to approve all contractor key personnel. If the FTC determines that a key person is unacceptable, the contractor shall replace the key person within 30 days.

In the event of key personnel departures, the contractor shall provide immediate and complete mission and functional coverage until replacements are available. These replacements are required within 30 days after departure of the key personnel. The contractor shall obtain FTC approval of the replacement key personnel.

C.1.6.3 Contractor Personnel

The contractor shall not employ any person who is an employee of the U.S. Government if employing that person would create a conflict of interest. Additionally, the contractor shall not employ any person who is an employee of the FTC unless such person receives FTC approval for such employment.

The contractor shall not employ persons to work on this contract if such applicant is a potential threat to the health, safety, security, general well being of other persons, or the operational mission of the FTC.

Pursuant to the CRC SOW, the contractor shall provide qualified personnel in sufficient quantities to perform the required tasks, including Consumer Information Specialists, project management, quality assurance, technical and support staff. The contractor shall ensure that the staff possesses the appropriate qualifications and skills required to perform the task and meet minimum qualifications and competencies. The FTC anticipates that up to fifteen percent (15%) of the telephone, internet and mail inquiries handled by the contractor will be in Spanish. The contractor shall provide sufficient

consumer information specialists, supervisors, quality assurance and management personnel who are proficient in English and Spanish (orally, in writing, or both) to handle this anticipated workload. The contractor shall cross-train the contact center and support staff to ensure sufficient qualified support is provided at all times to each of the supported activities. All contact center staff shall be situated in contractor-provided facilities with restricted access.

The contractor shall be responsible for the ongoing training of its employees to properly perform the duties and procedures necessary to provide the services required under this task. The contractor shall provide training to all of its employees about security matters relating to CIS. As part of the training procedure, the contractor shall obtain, maintain, and provide to the COTR, upon request, a signed FTC Non Disclosure Agreement from each of its employees assigned to this contract. The contractor shall include the steps it proposes to use to implement such training in its training plan. All individuals employed or retained by the contractor to fulfill the positions or duties described in this task shall be approved by the COTR for access to the FTC database systems, as provided under the security clearance procedures set forth in this SOW.

C.1.6.4 Additional Clearance Requirements for Contractor Personnel

C.1.6.4.1 Nondisclosure Agreement

Each individual employed or otherwise retained by the contractor to fulfill the contract positions or duties shall complete a Nondisclosure Agreement, set forth in CIS Technical Exhibit 5, and submit such completed form to the COTR at least five working days before that individual may begin work or be given access to any agency records, data, or information in connection with this contract.

C.1.6.4.2 Replacement Contractor Personnel

The contractor shall provide qualified replacements to the extent necessary to maintain performance under the contract. For example, pending resolution of any suitability issues, contractor personnel may be removed from contract duties; if such an individual is so removed, the contractor shall provide a qualified temporary replacement pending resolution of the suitability issue. The procedures set forth in this section shall apply to all individuals serving as replacement contractor personnel, who shall be required to submit all required forms within the time period(s) specified by these procedures, and shall agree to any resulting background investigations, before starting work or obtaining access to agency records, data, or information under the contract. Where appropriate, the FTC Security Officer may, in his/her discretion, waive these procedures in whole or part (see below, "Successor contractors").

C.1.6.4.3 Successor Contractors

If the contractor is subsequently replaced under this contract by another contractor, through assignment of the contract or otherwise, all individuals employed, carried over, or otherwise retained by the successor contractor to fulfill the contract positions or duties

shall be required to apply for and obtain suitability approval under the security procedures set forth in this section, regardless whether such individuals may have already obtained such approval when employed or otherwise retained by the previous contractor to fulfill the same or other contract position or duties. The FTC Security Officer, at his/her discretion, may waive this requirement, in whole or part, for any individual carried over from a previous contractor if the individual was determined suitable by the FTC within the last three years, or if the Security Officer otherwise determines that it is unnecessary for the individual to obtain a new suitability determination under these procedures.

C.1.6.4.4 Renewal of Suitability Determination

All individuals required to obtain a suitability determination under this contract shall obtain a new FTC suitability determination every five years; this requirement shall not be waived except in extraordinary circumstances, as determined by the FTC. Each such individual shall inform the FTC of changes in any information or documentation that was previously submitted by or on behalf of such individual to obtain clearance under this section. Failure to do so may result in immediate removal or disqualification of the individual from contract duties.

C.1.6.4.5 FTC Identification Card/Building Pass.

For contracts anticipated to exceed 30 days that require employees of the contractor to be present on a regular basis in any FTC building, the contractor shall, through coordination with the COTR, ensure that all such contractor personnel are issued FTC contractor identification cards/badges before they enter duty or have access to any agency records, data or information. The contractor shall ensure that its employees display their FTC contractor identification cards/badges at all times; and that all such cards/badges are returned to the COTR as contractor personnel are dismissed or terminated, and upon the expiration of the contract or applicable work order, whichever is earlier. All FTC contractor identification cards/badges shall have an expiration date of no more than one year from the issue date or from the contract expiration date, whichever period is shorter.

C.1.7 Third-party Requests for Access to Records

In addition to the section entitled “Handling of third-party requests for access to records” in the document “FTC Clauses and Special Provisions Applicable to this Order,” the contractor shall follow this guideline: All other types of voluntary or mandatory requests for access to materials, including inquiries from any media outlet, law enforcement, informant, other government agencies, cases of business-related identity theft, or Congress, except those requesting general information such as publications or brochures, shall be referred to the COTR for appropriate action within four hours of receipt.

C.1.8 Quality Control

After contract award, the contractor shall implement and follow the Quality Control Plan(s) that it submitted as part of its proposal, and that were approved by the FTC. The

minimum requirements for such plans are specified below in sections C.1.8.1, C.1.8.2, and C.1.8.3.

C.1.8.1 Description of the Inspection System

A description of the inspection system that will be used to evaluate all services listed in CIS SOW Section C.5 (Specific Tasks), CRC SOW Opt. 1.3 (Specific Tasks) and DNC SOW Opt. 2.1 (Specific Tasks). This description shall include, at a minimum:

- Methods to measure actual performance against performance standards.
- Control and audit procedures to identify areas adversely affecting contract performance.
- An approach to continuously improve quality and timeliness.
- A problem identification and resolution process and a method for monitoring corrective action.
- A system for recording, computing, accumulating, maintaining, and providing access to performance measurement data so that the contractor and FTC can use it for analysis and decision making.
- A method to identify and resolve user complaints.
- A method to monitor the accuracy and completeness of the data in the system.

C.1.8.2 Description of the Methods

A description of the methods to be used for identifying and preventing defects in the quality and timeliness of services performed.

C.1.8.3 Description of the Records

A description of the records to be kept to document inspections and corrective or preventative actions taken by the contractor under its quality control plan. These records of inspections and actions taken shall be kept by the contractor and made available to the contracting officer upon request throughout the contract performance period and for the period after contract completion until the final settlement of any claims under this contract.

C.1.9 Quality Assurance

C.1.9.1 Evaluation of Contractor’s Performance

As stated in each Performance Requirements Summary ("PRS"), the FTC will evaluate the contractor's performance under this contract. For those tasks listed in the PRS, the COTR or evaluators will follow the methods of surveillance specified in this contract.

The FTC will record all surveillance observations. When an observation indicates defective performance, the COTR will forward the observation to the contract manager or alternate(s), who shall initial the observation. The initialing of the observation does not necessarily constitute concurrence with the observation, only acknowledgment that he or she has been made aware of the defective performance. FTC surveillance of tasks not listed in the PRS or by methods other than those listed in the PRS may occur during the performance period of this contract. Such surveillance will be done according to standard inspection procedures or other contract provisions. Any action taken by the contracting officer as a result of surveillance will be in accordance with the terms of this contract.

Note that there is a separate PRS for each of the SOW's, and that the above paragraph is applicable to each PRS.

C.1.9.2 Performance Evaluation Meetings

The contracting officer may require the contract manager to meet with FTC personnel as deemed necessary. The contractor may request a meeting with the contracting officer when he or she believes such a meeting is necessary. At a minimum, the contract manager and other key personnel, and contracting officer (or other FTC personnel, as deemed necessary) shall meet quarterly to discuss the ongoing operation of the contract. The contractor shall prepare written minutes of such meetings, which shall be recorded in the contract file. The contract manager and the contracting officer shall sign the minutes or provide in writing their nonconcurrence within five calendar days following receipt of the minutes.

C.1.10 System and Data Ownership

During the performance of this contract, the contractor will create and maintain databases, information, and other materials that are used to support the various activities (e.g., customer service records, business rules, knowledge database, call flow diagrams, IVR scripts, FAQ, preformatted responses, business rules, training materials). The FTC retains ownership of all information resources: stored data, information, database structure, design and content of web pages, and other materials developed by the contractor in support of this contractor. The contractor shall retain ownership of the system (except for any items that may be furnished by the FTC), including all hardware and software. At the end of the performance period, all information resources developed in support of the contract shall be turned over to the FTC in its entirety.

C.1.11 Compliance with Applicable Laws and Regulations

The contractor shall ensure that all systems and services provided to the FTC under this contract comply with all applicable laws, statutes, regulations, and guidelines that govern the operation of systems by the FTC. The contractor shall also ensure that all systems and services provided to the FTC under this contract comply with all FTC mandated procedures, standards, and requirements.

As the FTC develops and implements new or modified policies and procedures either to comply with internal agency rules and procedures or to comply with applicable rules, regulations, statutes, or other binding obligations ("Additional Compliance Terms"), the FTC reserves the right to incorporate such Additional Compliance Terms into this Agreement. The contractor hereby acknowledges and agrees that such Additional Compliance Terms will become part of this contract. The FTC will provide the contractor with prior written notice regarding the date by which the contractor shall comply with each set of Additional Compliance Terms ("Compliance Date"). Failure to comply with the Additional Compliance Terms prior to the Compliance Date shall be cause for the FTC to immediately terminate this contract. In the event that the FTC terminates this contract because of the contractor's failure to comply with Additional Compliance Terms by the Compliance Date, the contractor shall be liable for such reasonable costs as may be associated with the FTC's efforts to procure a replacement contractor and associated systems and services.

The following is only a sample of some of the statutes, rules, regulations, and guidelines that the contractor shall comply with:

- Statutes. For example:
    - Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107-296, Title X, §§ 1001 to 1006, 89 Stat. 26
    - Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724
    - Paperwork Reduction Act of 1995, 44 U.S.C. §§ 3501-3520 (2006)
    - Clinger-Cohen Act of 1996, Pub. L. No. 104-106, Divisions D and E, 110 Stat. 186
    - Government Paperwork Elimination Act, 44 U.S.C. § 3504 (2006)
    - Management of Federal Agency Receipts, Disbursements, and Operation of the Cash Management Improvements Fund, 31 C.F.R. Part 206\
    - E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899

- Circulars, Memos, and Guidelines published by the Office of Management and Budget (OMB). For example:
    - OMB Memo M-06-16
    - OMB Circular A-130
    - Government Performance and Results Act Guidance, OMB Circular A-11, Part 2

- Circulars, Memos, Guidelines, Reports, and Recommendations published by the Government Accountability Office (GAO). For example:
    - GAO/AIMD-00-33, *Information Security Risk Assessment: Practices of Leading Organizations*
    - GAO/AIMD-98-68, *Executive Guide – Information Security Management: Learning from Leading Organizations*

- Circulars, Memos, Guidelines, Reports, and Recommendations published by the National Institute of Standards and Technology (NIST). For example:

- NIST Special Publication 800-9, *Good Security Practices for Electronic Government*
- NIST Special Publication 800-12, *An Introduction to Computer Security*
- NIST Special Publication 800-14, *Generally Accepted Principals and Practices for Security Information Technology Systems*
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- Federal Information Processing Standards – available at http://www.itl.nist.gov/fipspubs

C.1.12 Information and Physical Security

C.1.12.1 Information Security

The contractor shall comply with federal information systems security requirements as described by the National Institute of Standards and Technology (NIST) (see the Computer Security Resource Center website at www.csrc.nist.gov) and United States Office of Management and Budget Memorandum (OMB) M-06-16 (attached as CIS Technical Exhibit 6). The contractor shall comply with the FTC's specific guidelines pertaining to information systems security (CIS Technical Exhibits 7A – 7G: Enterprise Database Security Policy, Sensitive Information Handling Policy, Enterprise Encryption Policy, Server Security Policy, Password Policy, IT Audit Policy, and System Security Certification and Accreditation Policy).

The contractor shall provide protection for information and an information system that has been categorized in accordance with Federal Information Processing Standards Publication 199 as moderate impact. Authentication shall comply with that required for a system in which e-authentication assurance level "3" applies (see "E-Authentication Guidance for Federal Agencies" (OMB 04-04) and NIST Special Publication 800-63.) Authentication shall not be burdensome, and the contractor shall not develop a method of authentication that does not require users to download or install an application or file on their computers or networks.

In addition to the policies described above, adequate data protection includes the following discrete requirements, at a minimum:

- Encrypt all sensitive data in the database (at rest) and in transmission;

- Log all computer-readable data extracts and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required (OMB Memo M-06-16);

- Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access (OMB Memo M-06-16);

- Use a “time-out” function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity (OMB Memo M-06-16);

- Allow entry into the systems only to authorized individuals and only during authorized times;

- Maintain a history of password changes over a specified amount of time, including changes and lost passwords, and preclude the consecutive use of the same password;

- Passwords shall be non printing and non displaying. The system shall: (1) allow for the establishment of a specified period for password expiration to provide changes on a regular basis; (2) prohibit the user from reusing recent passwords; and (3) permit periodic password change, at the option of the user, and mandatory password change, at the option of the system administrator after a specific period of time;

- Maintain an audit logging capability to record access activity including the user ID, time and date of use, type of transaction, all log in/log out attempts, user submitted transactions, initiated transactions, system override events, and direct additions, changes or deletions to application maintained data;

- Limit the capability to select functions (e.g., data entry), as well as have the capability to define functional access rights (e.g., to modules, transactions, approval authorities) and data access rights (e.g., record, create, read, update, and delete) by assigned user ID, functional role, and user group. User profiles can be accessed, deleted, modified or changed by the system administrator;

- Allow the system administrator to restrict access to sensitive data elements by named user, user groups, or functional role;

- Alert and record when invalid access attempted or when the user ID limit is exceeded;

- Lock all accounts after five consecutive failed login attempts. The account shall remain locked until a system administrator unlocks it;

- Ensure that all users have unique user ID’s;

- Prevent users from simultaneous log-ins;

- Provide the ability for the FTC to query the audit log by type of access, date and time stamp range, user identification, user group, organization code, or access point;

- Internet and E-mail usage policy - Guidelines regarding appropriate Internet access and usage is implemented and enforced. Policies addressing access to and disclosure of electronic mail messages sent or received by employees using contractor’s corporate email system shall also be implemented and enforced. Such guidelines will inform employees that their privacy does not extend to their use of contractor-provided equipment or supplies; and

- Telecommunications systems - Provision of telecommunications security is sufficient to protect all incoming and outgoing calls and electronic contacts/responses, and all data collected from these activities, from unauthorized access or loss.

The systems and other electronic applications described in the SOW's shall be certified and accredited by the FTC Designated Approving Authority (DAA) prior to implementation. The contractor is responsible for preparing all certification and accreditation (C&A) documents described in the FTC System Security Certification and Accreditation Policy, coordinating the submission of such documents with the DAA, and correcting any deficiencies identified in the C&A process until full accreditation from the DAA is obtained.

The contractor must also continuously monitor the system and services provided under this SOW to ensure the security of the system. The contractor will provide the FTC with the following information:

- Incident and activity reports:
    - Immediate notice of any successful intrusions or exploits, along with any and all details regarding such incidents as the FTC may reasonably request;
    - Immediate notice of any hardware or software patches, along with any and all details regarding such patches as the FTC may reasonably request; and
    - Immediate notice of any hardware or software configuration changes, along with any and all details regarding such changes as the FTC may reasonably request.
- Monthly security report:
    - A checklist demonstrating compliance with applicable NIST standards and OMB Memorandum M-06-16, with detailed explanations for any noncompliance;
    - A checklist demonstrating compliance with applicable FTC guidelines found in CIS Technical Exhibits 7A – 7G, with detailed explanations for any noncompliance;
    - A checklist demonstrating compliance with the discrete requirements listed above, with detailed explanations for any noncompliance;
    - A detailed listing of the current patch level of all systems (including the availability of applicable patches and a schedule for when they will be applied);
    - A detailed explanation of any changes implemented to maintain compliance with the requirements in this section;
    - A detailed list of all attempted intrusions and exploits; and
    - A detailed hardware inventory and configuration.

For any security problems, including breaches, the contractor shall immediately notify the COTR and the FTC Chief Security Officer.

C.1.12.2 Physical Security

The contractor also shall be responsible for providing a physically secure facility for people, equipment, and documentation. All security requirements apply to the contractor facility, alternative facility, or any subcontractor facilities. When designing physical security measures, the contractor shall address factors including, but not limited to:

- Controlled access - All personnel who enter the facility shall be issued a badge or identification card. Employees have a permanent badge and approved visitors receive a temporary badge. In general, facility access is limited to: contractor personnel performing work under contract; authorized Government personnel; maintenance personnel or suppliers performing upkeep or repair of facilities or equipment; customer personnel visiting the site on official business; and personnel as approved jointly by the contractor and the FTC. The contractor must obtain FTC approval prior to granting either current or potential customers access to areas where FTC work is performed. Terminated employees shall have their badges removed and their accounts deactivated and/or deleted from any system access immediately upon termination. Proof of such removal shall be documented by the contractor and made available to the FTC upon request.

- Data and telecommunications center - The primary data and telecommunications center is secured through the use of key-code access with entrance granted only to those requiring access to this area on a regular basis to perform their normal job functions or who are escorted as in the case of visitors or technicians.

- Confidential information - Subsequent to the award of each contract, the FTC will provide the contractor with a listing of items it deems confidential in nature. Examples of such data include, but are not limited to, consumer names, addresses, and social security numbers. The contractor shall implement appropriate security measures to ensure such data is safeguarded in a manner consistent with those employed by the FTC. Examples of data security include locked file storage, confidentiality stamping, restricted system access, data encryption, restricted print options, and disposal by shredding.

- Proper notification – The contractor shall report all attempts made, whether successful or not, to breach the physical security of the facilities or primary data centers where the work is performed, or any related telecommunications and information systems that support each task. The contractor shall adhere to applicable agency IT Incidence Handling Procedures for reporting these intrusions, including escalation to Department of Homeland Security FedCIRC if necessary. **Such reports shall be made to the Government as soon as possible and in no event more than 24 hours after discovery of the incident.** In rare instances, the contractor may receive calls that threaten the well being of the Government and/or other personnel or property. The contractor shall ensure that procedures are in place to report the calls immediately to the appropriate law enforcement agency(ies) and the FTC.

The contractor shall provide the FTC with monthly status reports summarizing any attempted intrusions or exploits, along with all details regarding such incidents as the FTC may reasonably request.

C.1.13 Contingency/Disaster Recovery

The contractor shall develop and implement contingency/disaster recovery plans and procedures to address continuity of operations in the event of a shutdown or lapse in service for any reason. For outages that are not caused by a major disaster (e.g., system failure, network outage) the plans and procedures shall ensure that all attended and unattended services are restored to pre-outage performance levels by the contractor within four hours after report or discovery of the outage. For outages that are caused by a major disaster (e.g., tornado, hurricane, flooding), the plans and procedures shall ensure that all unattended services (e.g., websites, IVR, Hosted FAQ Service, Email Routing) be restored by the contractor to pre-outage performance levels within four hours after report or discovery of outage, and all attended services (e.g., inquiry response support, transcription, fulfillment) be restored by the contractor to pre-outage performance levels within 96 hours after report or discovery of outage. The contractor is responsible for restoring the services to their primary service location(s) upon correction of the outage problem.

All contingency/disaster recovery plans and procedures shall comply with the physical and information security guidelines outlined in the preceding section.

C.1.13.1 Program Operations Recovery

In the event of periodic or catastrophic failures that restrict or terminate program operations, the design of CIS and, if applicable, the contact center infrastructure, the communications network servicing the FTC, and the National Do Not Call Registry, shall include sufficient redundancy to allow normal business operations to continue with minimal disruption and inconvenience to customers for all access channels.

C.1.13.2 Data Recovery

When designing disaster recovery plans for data recovery, the contractor shall address factors including, but not limited to:

Backup routines - The ease and frequency of which backup routines are conducted and the ability to backup data on remote servers/processors.

Effectiveness - The degree to which data can be compressed for backup purposes and the ability to perform unattended backups on high-density/high-capacity storage devices.

Operational impact - The time that is required to complete backups and the need to remove users from the system to conduct backup routines.

Data integrity - The methods of maintaining data integrity so that completed transactions are not lost due to outages, system failures, etc. In long-running transactions, such as

when an information specialist needs to navigate several screens of data entry, there should be interim checkpoints that save the transaction so that it may be re-entered from the last checkpoint if the transaction was not completed prior to the failure.

Data recovery - The methods of restoring data from backup in the event of a failure (e.g., commercial power failure, system or hardware failures).

Simulated tests - Regularly scheduled simulated tests shall be conducted for purposes of preparing the staff and assessing the plan's viability.

C.1.13.3 Voice Recovery

When designing disaster recovery plans for the communications network, the contractor shall address factors including, but not limited to:

Network routing - If an individual facility should become inaccessible, a sufficient communications network shall be in place to allow for forwarding of customer calls to one or more alternate facilities. If the outage is brief, the network shall resume normal call routing as soon as the primary facility is operational again.

Operational impact - Documented policies shall exist for assuming workload from an incapacitated facility for immediate, short-term, and long-term relief.

Simulated tests - Regularly scheduled simulated tests shall be conducted for purposes of preparing the staff and assessing the plan's viability.

C.1.13.4 Notification Process

The contractor shall implement procedures for communicating to the COTR or alternate disaster-related issues that inhibit system or contact center operations. Such procedure shall include an escalation process defining various stages of issue severity and the notification level appropriate to each.

C.1.14 Privacy Act of 1974

When an agency is acquiring information technology, the FAR provides generally that the agency must specify appropriate information security policies and requirements to be followed by the contractor. See 48 C.F.R. (FAR) 39.101(d). Such policies and requirements are set out throughout this document. See, e.g., section C.1.12 (Information and Physical Security). In addition, when a contract will include the design, development or operation of systems of agency records within the meaning of the Privacy Act of 1974 (5 U.S.C. 552a), as in this case, the FAR also requires that the contract specifically address protection of privacy in accordance with that Act and corresponding FAR provisions. See FAR 39.105 (privacy) and FAR Part 24 (protection of privacy and Freedom of Information Act).

C.1.14.1 Privacy Act System of Records: CIS

The Privacy Act system of records corresponding to CIS records is currently designated FTC-IV-1 (Correspondence Control System—FTC), http://www.ftc.gov/foia/sysnot/iv-1.pdf (CRC or CIS "system notice"), which may be legally amended at any time by the FTC without prior notice or approval of the contractor. The contractor understands and agrees that records collected, maintained, and retrieved about individuals within the meaning of the Act by the contractor for the FTC in the CIS system shall be subject to the Privacy Act requirements of this contract, whether or not those records are specifically described or enumerated in the above-cited system notice, as modified or superseded at any time.

Specifically, CIS contains consumers' personal information, which may include: first and last name; street address; city; state; zip code; email address; date of birth or age range; and telephone number(s). For two categories of complaints – identity theft-related complaints and complaints related to the accuracy of the consumer's credit report – CIS permits consumers to provide a Social Security number. CIS also collects and maintains the subject matter of consumers' complaints (a 2,000-character free text "comments" field) – which may contain additional sensitive personally identifiable information or sensitive health information - and information regarding the companies, entities, or individuals about which the consumer is complaining.

C.1.14.2 Privacy Act System of Records: DNC

The Privacy Act system of records corresponding to DNC records is currently designated FTC-IV-3 (National Do Not Call Registry System–FTC), www.ftc.gov/foia/031103privactDNC.pdf (DNC "system notice"), which may be legally amended at any time by the FTC without prior notice or approval of the contractor. The contractor understands and agrees that records collected, maintained, and retrieved about individuals within the meaning of the Act by the contractor for the FTC in the DNC system shall be subject to the Privacy Act requirements of this contract, whether or not they are specifically described or enumerated in the above system notice, as modified or superseded at any time.

Specifically, the DNC registry contains consumer telephone numbers obtained through the registration process. As part of the telemarketer subscription process, individual name, social security number, and credit information may be obtained. As part of the DNC complaint process, these records may contain personally identifiable information.

C.1.14.3 Privacy Act System of Records: Identity Theft

The Privacy Act system of records corresponding to identity theft (IDT) records is currently designated FTC-IV-2 (Identity Theft Complaint Management System-FTC), http://www.ftc.gov/foia/031103privact1974.pdf (IDT "system notice"), which may be legally amended at any time by the FTC without prior notice or approval of the contractor. The contractor understands and agrees that records collected, maintained, and retrieved about individuals within the meaning of the Act by the contractor for the FTC in

the IDT system shall be subject to the Privacy Act requirements of this contract, whether or not those records are specifically described or enumerated in the above-cited system notice, as modified or superseded at any time.

Specifically, the IDT system contains individuals' (victims, suspects, and persons reporting on behalf of victims) personal information, which may include: first and last name, address, telephone number, fax number, date of birth, social security number, credit card numbers, e-mail address, and other personal information extracted or summarized from the individual's complaint. The IDT system also collects and maintains the subject matter of victims' complaints (currently, a 2,000-character free text "comments" field) which may contain additional sensitive personally identifiable information or sensitive health information.

C.1.14.4 Privacy Act Requirements for Systems of Records Designed, Developed or Operated by the Contractor

The contractor shall comply with FAR 52.224-1 (Privacy Act notification) and 52.224-2 (Privacy Act), which are incorporated by reference here and elsewhere in this document. The latter FAR clause explicitly requires that the contractor comply with the Privacy Act and all implementing agency rules and regulations.

For purposes of this contract, such Privacy Act rules and regulations shall include, but are not limited, to FTC Operating Manual, ch. 15.10 (Privacy Act procedures), available online at: http://www.ftc.gov/foia/ch15confidentialityandaccess.pdf, and shall also include compliance with any other agency policies, procedures, or changes that may be developed or issued to the FTC's own employees, consultants, or contractors during the performance of this contract. In addition, applicable Privacy Act rules and regulations shall include, but not be limited to, the FTC's Rules of Practice, particularly Rule 4.13 (Privacy Act), 16 C.F.R. 4.13, and any applicable Privacy Act guidance issued by the OMB (e.g., OMB Circular A-130, Appendix I).

The contractor shall pay particular attention to the Act's requirements for verifying identity, purpose, and authority of the requester before any disclosure of system records, accounting (tracking) of disclosures, protecting the security and integrity of system records from threats and hazards (see below), and providing Privacy Act notices to individuals, the text of which shall be supplied by the FTC, when collecting information from such individuals, whether in writing (e.g., notice included on paper or electronic forms used to collect complaints or other data from individuals, etc.) or orally (e.g., recorded or live oral notice given over the telephone to individual callers).

Certain Privacy Act responsibilities, such as the publication of system notices in the Federal Register, shall not be the contractor's responsibility. As explained elsewhere in this document, with respect to disclosure of system records, **neither the contractor nor its employees or agents, as explained elsewhere in this document, shall have any duty or authority to disclose system records unless expressly authorized by the contract and/or approved by the appropriate designated FTC officials or employees.** Should the contractor need clarification of any of the agency's Privacy Act rules and

regulations, the contractor, unless otherwise provided in the contract, shall consult with the COTR, who shall make best efforts to obtain such clarification from FTC legal counsel or other appropriate individual(s). To comply with the Act, the contractor shall also be required to provide sufficient system data, at no additional cost, to the FTC in formats to be specified by the FTC, for the agency to fulfill its own reporting or other compliance, monitoring, or accounting duties under the Act. The cost of complying with these requirements shall be included in the total contract price and shall be borne exclusively by the contractor.

C.1.14.5 Additional Privacy Act Requirements for IT Service or IT Support Service Contracts

To the extent this contract shall be for the design, development, or operation of a Privacy Act system of records using commercial information technology services or information technology support services, the following additional provisions shall also apply, see FAR 39.105:

(a) Agency rules of conduct that the contractor and the contractor's employees shall be required to follow: These rules of conduct include, but are not limited to: FTC and other rules, regulations, and policies noted above relating to the Privacy Act; other FTC relevant internal privacy and/or information technology policies or guidance; any policies or guidance implementing FISMA, Homeland Security, and NIST information security requirements or guidance; and the applicable privacy policies and privacy impact assessments posted on the FTC's Web sites pursuant to the EGOV Act of 2002. Copies or links to such information shall be provided upon request. To the extent that such information is publicly available, the agency's delay or failure, if any, to provide requested copies or links shall not excuse the Contractor's delay or failure, if any, to comply.

(b) Anticipated threats and hazards that the contractor must guard against: In accordance with NIST Federal Information Processing Standards (FIPS) Publication 199, the agency has categorized CIS, IDT, DNC, and the information contained therein, as "moderate impact" system[s] in terms of risk. They also have been designated as "major applications" in accordance with OMB A-130. Threats and hazards to CIS, IDT and DNC system records include, but are not limited to: unauthorized access, disclosure, alteration or removal by contractor employees or others; pretexting (i.e., internal or external attempts to obtain unauthorized access through methods designed to evade required identity verification procedures); malicious viruses, spyware, phishing, cookies or similar threats where records are maintained, retrieved, or transmitted or otherwise managed through online methods (e.g., access or dissemination through Web sites or servers) or in whole or part through online communications (e.g., e-mails or electronic file exchanges between contractor and consumers or other individuals regarding system records); improper commingling; accidental or willful destruction; temporary or permanent loss or impairment of information collection or access to records in the event of electrical, software, or other system failure or catastrophic event, etc.; vulnerabilities, if any, in processes for remote physical, logical or electronic access or transfer (e.g., Web-

based access to DNC records by telemarketers, etc.). **NOTE: The preceding list is not exhaustive.** The contractor is expected to follow applicable requirements and industry best practices, as also described elsewhere in this document, to anticipate, identify, and implement reasonable safeguards against threats and hazards to system records. As provided in FAR 52.239-1 (Privacy or Security Safeguards), which is incorporated by reference, if new or unanticipated threats or hazards are discovered by either the FTC or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(c) Safeguards that the contractor must specifically provide: The contractor is required to provide all safeguards described elsewhere in this document to protect the security and integrity of the relevant system and records contained therein. To the extent not otherwise specified or required in this document, the contractor's proposal shall including a completed Self-Assessment Questionnaire under applicable NIST standards. See NIST Draft SP 800-26, Revision 1, *Guide for Information Security Program Assessments and System Reporting Form*, [Reference questionnaire format to be used in http://csrc.nist.gov/publications/drafts/Draft-sp800-26Rev1.pdf] NIST 800-26 assesses information security assurance of the offeror's internal systems security. This assessment is based on the Federal IT Security Assessment Framework and Draft NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*. [Reference: http://csrc.nist.gov/publications/drafts/800-53-rev1-clean-sz.pdf.] The contractor shall update this questionnaire annually following award in accordance with FISMA and OMB policy. This questionnaire shall be subject to FTC approval. Questionnaires deemed to be insufficient may be deemed non-responsive and may render the proposal ineligible for award. Likewise, to the extent not otherwise specified or required in this document, the contractor's proposal must include a draft Information System Security Plan (ISSP) using the most current template in Appendix A of NIST SP 800-18, Revision 1, *Guide to Developing Security Plans for Federal Information Systems*, which is available at http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf. The draft ISSP must be commensurate with the size and complexity of the contract performance requirements. This plan shall be subject to FTC approval for sufficiency and consistency with FISMA and other applicable laws, regulations and policies. The contractor must update and resubmit its ISSP every three years following award or, in any event, when a major modification is made to the system.

(d) Requirements for a program of Government inspection during performance of the contract that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards: To the extent not otherwise incorporated into this document elsewhere, FAR 52.239-1, Privacy or Security Safeguards, is hereby incorporated by reference. This clause provides, among other things, that the contractor shall afford the FTC access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases to the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of data maintained on the FTC's behalf. As noted earlier, this clause also requires notice of any new or unanticipated threats or hazards are discovered by either the FTC or the contractor, or

if existing safeguards have ceased to function. The contractor's ISSP shall include reasonable procedures for ensuring the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

(e) To the extent not required by the monthly security report described in section C.1.12.1, the contractor shall provide a monthly report detailing compliance with subsections (a), (b) and (c) herein.

C.1.14.6 EGOV Requirements for Privacy Policies and Privacy Impact Statements (PIA's)

The contractor shall be required to provide full and timely assistance to the FTC, including requested data, reports or other information in formats requested by the FTC, in the preparation of any required privacy policies for any websites relating to either the CIS, IDT or DNC systems and privacy impact statements for such systems, as required by section 208 of the EGOV Act of 2002. The contactor should review the relevant privacy policies and privacy impact statements posted on the FTC Web site as guidance in construing this requirement. See, e.g., (http://www.ftc.gov/os/2004/11/041104coninfosysprivimpassess.pdf) (CIS PIA); http://www.ftc.gov/ftc/privacy.htm (FTC privacy policy, applicable to CIS and DNC).

C.1.14.7 Year 2000 Compliance

To the extent that this contract will require the contractor to perform date/time processing involving dates subsequent to December 31, 1999, the contractor's information technology must be Year 2000 compliant. See FAR 39.106.

C.1.15 Hours of Operation

Except as otherwise set forth in this contract or for scheduled maintenance, the contractor shall take reasonable steps to ensure web based access to the system 24 hours per day, seven days per week, 52 weeks per year. Scheduled maintenance shall be approved in advance by the COTR, and the contractor shall make every effort to minimize such maintenance to the least amount of time necessary and perform it during off-peak periods (i.e., minimal system usage). For those tasks that may involve a live operator (e.g., CRC SOW), the contractor shall provide such service Monday through Friday, except federal holidays, between 9:00 am and 8:00 pm Eastern time.

Unless directed otherwise by the Government, the contractor shall provide an automated interactive voice response service to enable telephone callers to access information twenty-four hours a day, seven days a week (24 x 7) for each of the programs supported. The automated service shall provide an option for the callers to obtain live assistance from qualified contractor personnel during the hours between 9:00 am and 8:00 pm Eastern time, Monday to Friday, except federal holidays.

To accommodate callers who call just prior to the 8:00 pm closing time, the contractor shall make reasonable accommodation in extending the closing time of the center by a

few minutes to allow calls that have entered the normal business hour automated voice response service menu prior to the closing time to progress through to the contact center staff for assistance.

C.1.16 Records

The contractor shall be responsible for creating, maintaining and disposing of only those government required records that are specifically listed in this SOW. If requested by the contracting officer or COTR, the contractor shall provide the original record, or a reproducible copy of such record, within three working days of receipt of the request.

C.1.17 Compliance with Section 508 of the Rehabilitation Act of 1973

To the extent that this contract involves the development, procurement, maintenance or use of electronic and information technology by a federal agency, it is subject to the requirements of Section 508 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 794d, and the disability access standards issued thereunder by the Architectural and Transportation Barriers Compliance Board ("Access Board"), 36 C.F.R. Part 1194. In particular, when members of the public seek information or services from a federal agency, Section 508 requires that the agency ensure that technology developed, procured, maintained or used by the agency allows individuals with disabilities to have access to and use of information and data that is comparable to the access and use provided to members of the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency; in such cases, individuals with disabilities must be provided alternative means of access that allows them to use the information and data.

C.1.18 Project Plan

As part of its solicitation, the contractor shall include preliminary project plans for each SOW. At a minimum, the project plans shall include a schedule for milestones. For the CIS SOW specifically, the project schedule shall outline the approximate timing for the phases detailed in section C.6.

C.2 DEFINITIONS AND ACRONYMS

C.2.1 Definitions

Completed registration request: Each successful integration into the national registry of all information provided by a consumer as set forth in DNC SOW, Sub Task 1-1, or each successful request by a consumer to remove a telephone number from the registry or re-register a telephone number, as set forth in the DNC SOW, Sub Task 1-4.

Consumer Sentinel Data Mart: A data warehouse of all records that are stored in the Consumer Information System that is used as the query and reporting repository for the Consumer Sentinel Network. The CSDM also houses the National Do Not Call Registry complaints.

Crosswalk: Mechanisms to upload bulk complaints into CIS (also called imports), request bulk downloads of complaints (also called exports), and administer the quality assurance (QA), scheduling, logging, and notification aspects of the process.

Defective service: A service output that does not meet the standards of performance requirement specified in the contract for that service.

Normal business hours: 9:00 am to 8:00 pm Eastern time, Monday through Friday, 52 weeks per year, except for federal government holidays.

Organization code: The unique identifier of a Consumer Sentinel Network member, data contributor, or data receiver.

Performance requirement: The point that divides acceptable and unacceptable performance of a task according to the Inspection of Services clause. It is the maximum percentage of defective service that is acceptable.

Reference number: A unique system generated identification number.

Valid processed call log records: Each call log record that is included as part of a deliverable (or report) that is provided to the FTC pursuant to the DNC SOW, Task Six, Opt. 2.7, and which is accepted by the FTC.

Valid processed contact center complaints: Information provided by a consumer that is gathered by the contact center contractor pursuant to the CRC SOW, Sub Tasks 1.1 and Task 2, and successfully loaded into the CIS database.

Valid processed DNC complaints: Information, provided by a consumer indicating a problem concerning compliance with the FTC's do not call requirements of the Telemarketing Sales Rule, that is gathered by the contractor pursuant to the DNC SOW, Sub Task 4-1 and successfully loaded into the CIS database. The term does not include those contacts by a consumer which are determined to be invalid complaints, as outlined in the DNC SOW, paragraph Opt.2.5.1.1.

C.2.2 Acronyms

ACRONYMS	DEFINITIONS
BCP	Bureau of Consumer Protection
BO	Business Objects
CRC	Contact Center Services
CIS	Consumer Information System
CMS	(Congressional) Correspondence Management System
CO	Contracting Officer
COTR	Contracting Officer’s Technical Representative
CPS	Consumer Planet Sentinel
CRC	Consumer Response Center
CS	Consumer Sentinel

CSDM	Consumer Sentinel Data Mart
CSN	Consumer Sentinel Network
DNC	Do Not Call (National Do Not Call Registry)
DOD	Department of Defense
FAR	Federal Acquisition Regulations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
IDT	Identity Theft
ITM	Office of Information and Technology Management
ISSP	Information System Security Plan
IVR	Interactive Voice Recognition
NIST	National Institute of Standards and Technology
NTL	National Tape Library
OMB	Executive Office of the President, Office of Management and Budget
PIA	Privacy Impact Assessment
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
SOW	Statement of Work
TSR	Telemarketing Sales Rule
USPS	United States Postal Service
XML	Extensible Markup Language

C.3 GOVERNMENT FURNISHED ITEMS

The FTC will provide the services and materials listed in this section to the contractor for use in performing the requirements of this SOW.

C.3.1 Websites

The FTC will provide the contractor with the URL(s) for the contractor's website(s) to be used for: (1) data contributor upload (CIS SOW Sub Task 1.4); (2) FTC and law enforcement access to the system (CIS SOW Task 2) (https://cs.sentinel.gov); and (3) data receiver bulk download (CIS SOW Sub Task 2.4). (As stated later, the contractor may use the same website for all of these functions.) The FTC also will provide the URL's for the contractor's websites for collecting consumer data (CRC SOW Sub Task 1.1). In addition, the FTC will provide the contractor with the URL for the contractor's website to be used for consumer Internet registration requests (DNC SOW, Sub Task 1-1, Paragraph Opt.2.2.1.3) and consumer complaints (DNC SOW, Sub Task 4-1). The URL to be used is www.donotcall.gov.

C.3.2 Telephone Numbers

The FTC will provide the contractor with the toll-free telephone number, but not the long distance service, to be used by CIS users for requests for customer service. The telephone number is 877-701-9595.

The FTC also will provide the toll-free telephone numbers, but not the long distance services, for consumers to use. The telephone numbers are 877-382-4357 (877-FTC-HELP), 877-438-4338 (877-ID-THEFT), 877-987-3728 (kNOw Fraud), and 866-653-4261 (hearing impaired (TTY)). The contractor shall either, as an agent of the government, make use of FTS 2001 phone service or provide their own service at comparable pricing rates.

The FTC also will provide the contractor with the toll-free telephone numbers, but not the long distance service, to be used by consumers to access the national registry. The telephone numbers are 1-888-382-1222 (voice), 1-800-382-1222 (voice), and 1-866-290-4236 (TTY).

C.3.3 Translations for Complaint Forms

The FTC will provide the contractor with translations for the econsumer.gov complaint forms and update to those forms. Currently, the FTC has translations in the following languages: French, German, Japanese, Polish, and Spanish (Japanese and Polish versions have not been deployed).

C.3.4 Materials and Publications

The FTC will furnish pertinent information to the contractor for use in the performance of this task. Examples of information that will be furnished include the following:

a. Initial content for knowledge database;
b. Federal statues, rules, and regulations enforced by the FTC;
c. Business rules, response formats, guidelines, and preformatted responses;
d. Existing IVR call flow and scripts;
e. Escalation procedures and guidelines;
f. FTC IT systems security policy and guidelines;
g. Reference materials;
h. Information packets, publications and forms for fulfillment; and
i. URL links to web based versions of FTC publications.

The contractor shall be responsible for inquiring before and throughout the life of the contract regarding any relevant changes in such materials. For any materials to be distributed by the contractor to the public, the contractor shall be responsible for stocking adequate supply and submitting resupply requests on a timely basis to ensure continuous availability.

C.3.5 Training

The FTC will provide training in the statutes and rules administered by the agency, including Privacy Act requirements. In addition, the FTC will provide update training and briefings on an as-needed basis. The FTC shall provide initial training for contractor personnel before the contract start date. The FTC shall not be responsible for training after this initial training period except in cases where initiation of a new project is authorized by the COTR, or where changes in law or consumer education materials require training updates.

C.3.6 Cash Management System

The FTC will provide the contractor, via the United States Treasury, with a cash management system for telemarketer user fee transactions. See DNC SOW, Sub Task 2-3, Paragraph Opt.2.3.3.1.

C.4 CONTRACTOR FURNISHED ITEMS AND SERVICES

Except for those items specifically stated in section C.3 as government furnished, the contractor shall furnish everything needed to perform the requirement of this contract. All items and facilities provided shall be located within the contiguous 48 states. If the contractor requires FTC personnel for any system testing, the contractor shall provide facilities within the metropolitan Washington, D.C. area to do so.

C.5 SPECIFIC TASKS

Sections C.5.2 – C.5.8 are applicable to the CRC SOW and DNC SOW as well. The remainder of this section (C.5.1 and C.5.9 – C.5.11) is applicable only to CIS.

C.5.1 General Information

The contractor shall develop, implement and operate a storehouse of consumer data relating to the FTC's consumer protection mission. The specific tasks in the CIS SOW are divided into three main parts: (1) collect, process and store consumer data; (2) provide web based access to the data for the FTC and law enforcement; and (3) provide reports.

C.5.2 Continuous Improvement

The contractor shall implement a continuous improvement program to identify and implement improvements to the services, processes, and systems that are provided under this contract. Improvements shall include modifications that improve the end-user experience, result in lower costs to the FTC, or result in increased operational efficiency. Improvements also shall include modifications necessitated by: (1) the incorporation into the contract of Additional Compliance Terms, as that term is defined in section C.1.11; (2) any new or substantially revised statue, rule, regulation or guidelines that were not reasonably anticipated with which the contractor must comply; (3) any significant

changes to the information and physical security and Privacy Act of 1974 requirements as described in sections C.1.12 and C.1.14; (4) a significant increase in CIS concurrent users; (5) updates to and new versions of web browsers as referenced in section C.5.4; (6) any upgrades to Pay.gov, as described in Opt.2.3.3.7; and (7) as requested by the FTC, enhancements of functions, websites, online forms, graphic interfaces, tutorial tools, help systems, quality assurance systems, telecommunications tools and systems (including, but not limited to, IVR, AVR, TTS, voice recognition service, etc.), and reporting requirements not already included in the SOW. The contractor shall submit such improvements to the COTR for approval, prior to implementation. In the event that the FTC does not approve of a particular improvement, then that improvement will not be implemented by the contractor. Payment for the implementation of these improvements is described in the Performance Requirements Summary for each SOW.

C.5.3 Web Based Architecture

The contractor shall develop and provide a system that utilizes web-based best practices and industry standards.

C.5.4 FTC Review of Websites, Online Forms and Other Deliverables

All websites, online forms, function screens (e.g., query, reports, etc.), tutorial tools, IVR scripts and recordings, and help systems shall be submitted for FTC review, feedback and approval of design, content and functionality.

C.5.5 Compatible Browsers

For all web based features, the system shall be compatible with and have complete functionality using the latest version of the industry standard browsers and two previous versions (e.g., Firefox, Internet Explorer, and Netscape).

C.5.6 User Administration

The contractor shall provide a method to grant and terminate access to the system and assign, modify, and withdraw privileges to ensure that authorized users have secure, transparent, and reliable access to resources in accordance with FTC security policies. The COTR or person designated by the COTR will authorize access for individual users. The contractor shall provide each approved user with a unique user ID and password for access to the system. All account metadata shall be maintained indefinitely. However, accounts may be deactivated.

C.5.7 Machine Readable Privacy Policies

The contractor shall make the Privacy Policies on the FTC's websites available in machine readable formats, in accordance with the Platform for Privacy Preference Project (P3P) standards.

C.5.8 Section 508 Toggle Capability

For all interfaces that are non-public (e.g., for law enforcement or the contact center counselors), the system shall have the capability to toggle section 508 compatibility functions on and off, depending on user preference. The default setting shall be for section 508 compatibility to be off. The capability to toggle on section 508 capability shall itself be apparent to disable users and section 508 compliant.

C.5.9 Task One: Collect, Process and Store Consumer Data

The contractor shall develop and provide: (1) integration of data currently housed in CIS/CSDM; (2) integration of National Do Not Call Registry (DNC) complaints; (3) integration with the CRC call center contractor's customer relationship management (CRM) application; (4) a method to integrate consumer data from other organizations; (5) a database to maintain the consumer information; and (6) a method to update certain metadata values.

C.5.9.1 Sub Task 1.1: Integrate Data Currently in CIS/CSDM

The contractor shall transfer and load records from the current CIS/CSDM into the new database. The transfer shall maintain the integrity of the data – no data may be lost, altered or added. All records shall maintain their CIS/CSDM unique reference numbers and original load date and, where applicable, time.

C.5.9.2 Sub Task 1.2: Integrate DNC Complaints

The contractor shall develop and provide a system that automatically loads into the database consumer complaints transferred from the FTC's National Do Not Call Registry contractor. The DNC complaints will be transferred on a daily basis using XML and WSDL. The FTC will not perform QA on these complaints before they are loaded into the database.

All DNC complaints shall be assigned the "National Do Not Call Registry" product/service code and organization code. In addition, all DNC complaints shall have comments as provided by the FTC.

The contractor shall integrate the DNC complaints with the requirements under Task One.

C.5.9.3 Sub Task 1.3: Collect and Process Consumer Data via Integration with Contact Center CRM Application

C.5.9.3.1 Permit Access by Call Center Information Specialists

The contractor shall develop and provide a system that permits secure remote access by contact center information specialists. Information specialists shall have access to complaints that were entered by the contact center or are web based complaints. The system shall be capable of handling up to 200 concurrent contact center users.

Currently, the contact center contractor runs the CIS application (Oracle database) from its own server. The FTC connects with the contact center utilizing a frame relay and transmits data through formatted messages using Oracle stored procedures.

When this contract is fully implemented, the FTC will no longer utilize a client-server application. The FTC envisions that the contractor's system eventually will need to communicate with a contact center data collection system or CRM through the use of XML and web services. Accordingly, the contractor shall ensure that its system is capable of connecting with a call center system based on a web service model.

If necessary, the system shall be capable of accepting user authentication credentials from a contact center CRM application. The system shall be capable of interoperating with a CRM application.

C.5.9.3.2 Insertion of Records

All records received from the contact center shall be immediately inserted into the database. Upon record submission, a reference number shall be generated immediately and transmitted to the contact center. Each record shall contain the appropriate organization code, the user ID, the date and time that it was loaded into the database, and any other minimum system generated data. A detailed listing of the number of records inserted monthly by the contact center is attached as CRC SOW Technical Exhibit 1.

C.5.9.3.3 Update of Records

The system shall permit contact center information specialists to retrieve and update any web based complaints, and records that previously were entered by the contact center. The contractor shall provide the contact center with one of the following: (1) search function described in Task Two; or (2) interoperability between the system and the contact center's CRM application search function. An updated record shall contain the date(s) and time(s) that it was modified, the data field(s) that were modified, the previous value(s) of modified data fields, and the user(s) who modified the record.

C.5.9.3.4 Integration

The contractor shall determine how best to collect and process consumer data collected by the contact center.

C.5.9.4 Sub Task 1.4: Import Records from External Data Contributors

The contractor shall develop and provide a system that will accept and integrate records from external contributors (crosswalks) and, when necessary, provide means for the FTC to QA the data before it goes into the database. Data on imported records is contained in CIS Technical Exhibits 9 and 10.

C.5.9.4.1 Contributor Data Formats and Record Forms

Currently, the data from external contributors is formatted in the following ways: (1) parsed XML SOAP data transfers; (2) text file – comma delimited; (3) fixed format; and (4) MS Excel. The system shall be capable of receiving data in these formats, as well as XML.

Currently, the contributors' data is received via email and CD. The system shall be capable of receiving data by these methods of transmission, as well as through a web service (in either batched files or individually in real-time).

C.5.9.4.2 Map Contributor Data to FTC Fields

For new contributors, the FTC will provide the contractor with the initial mapping of the contributor's data to the FTC data fields and values. The contractor shall be responsible for the technical mapping. Likewise, when an existing contributor alters the format of its data, the FTC will revise the mapping accordingly, and the contractor shall provide the technical mapping. All new and revised mappings shall be tested. The contractor shall obtain the FTC's final approval of the mapping before loading data into the system. (For any contributors providing data at the time of contract award, the FTC will provide its current crosswalk mappings.)

Where multiple contributors provide data in such a way that the same mapping can be used for each (e.g., identical data fields and identical values), the contractor shall treat the imports collectively as one initial import (e.g., currently, the Better Business Bureaus). Each import using the same mapping thereafter shall be treated as a subsequent import.

C.5.9.4.3 Secure Website for Data Transfer

The contractor shall develop and provide a secure website that will permit data contributors to upload their mapped data in an asynchronous manner into a crosswalk queue for QA. The contractor shall take into account that the speed of contributors' connections to the internet will vary. All such contributors will have had their data mapped to FTC data fields and values pursuant to section C.5.9.4.2. The website shall be password protected and accessible only by data contributors approved by the FTC. The website can be the same one that law enforcement uses to access the Consumer Sentinel Network (https://cs.sentinel.gov) or the same one used by data receivers (see Sub Task 2.4).

Data contributors shall receive notification of successful data uploads into the crosswalk queue.

C.5.9.4.3.1 User Administration for Data Contributors

The FTC will approve data contributor organizations. The COTR or person designated by the COTR will authorize access to the secure website for data transfer for users within data contributor organizations. The contractor shall provide each user with a user ID and

password for access to the system. Data contributor users will have access only to the secure contributor website.

C.5.9.4.4 Quality Assurance of Import Data by FTC

The contractor shall provide a mechanism that permits the FTC to perform QA for records received from an external data contributor prior to uploading them into the database. The mechanism shall provide the FTC with the option to approve, modify or reject import files.

C.5.9.4.5 Upload Contributor Records into the Database

Upon direction by the FTC, the contractor shall upload the approved records in the import file. The contractor shall log processing errors and store records that contain invalid data so those records can be reviewed and processed separately, if necessary.

C.5.9.4.6 Retention of Records

The contractor shall retain in a secure manner the original data contributor files for a period of 90 days after records from that file have been successfully uploaded into the database pursuant to section C.5.9.4.5. At the end of this retention period, the contractor shall purge these files, unless directed otherwise by the FTC. If the files were transmitted via CD, DVD or similar transportable media, the media shall be destroyed per FISMA standards.

C.5.9.5 Sub Task 1.5: Maintain Consumer Information in a Database

The contractor shall develop and provide a secure database that stores, in individual records, the information collected from consumers and any other system generated data. (In addition to fields noted in the technical exhibits, the FTC will add some additional fields of information to be collected after contract award. Two fields in particular are the "language of the transaction" (with corresponding values) and "county.")

C.5.9.5.1 Minimum System Generated Data

At a minimum, each record loaded into the database shall contain a reference number, an organization code, the date and time that it was loaded into the database, contact type, product/service code or identity theft subtype, and identification of the user creating or updating the record. The identification numbers shall follow sequentially from those records currently housed in CIS/CSDM. Each record also shall indicate its category (e.g., general, DNC, IDT or other). For an updated record, it shall contain a log of the date(s) and time(s) that it was modified, the data field(s) that were modified, the previous value(s) of modified data fields, and the user(s) who modified the record.

C.5.9.5.2 Retention of Data

Information housed in the database shall be retained indefinitely, unless otherwise directed by the FTC.

C.5.9.6 Sub Task 1.6: Add, Modify or Delete Values

The contractor shall add, modify or delete certain metadata values (e.g., product/service codes, statute/rules, law violations, topic codes, etc.) pursuant to the FTC's request. After contract award, the FTC may request such changes once per month, in addition to four ad hoc requests per year.

The system shall provide for an automated export of these values to the call center contractor's system each time there is a change to the values.

C.5.10 Task Two: Law Enforcement Access to the Consumer Data

The contractor shall develop and provide a system that: (1) permits law enforcement to access the data; (2) allows users to retrieve data via structured queries and parameterized reports; (3) provides certain users with direct access to the data to perform ad hoc reporting; (4) downloads batch files for export; (5) securely exchanges data with law enforcement networks; (6) contains web pages for reference materials; and (7) offers customer support.

C.5.10.1 Sub Task 2.1: Permit Web Access by Authorized Law Enforcement Users and Other Data Receivers

The contractor shall develop and provide a system that permits secure, web based access by FTC staff and authorized law enforcement users. The system shall be capable of handling up to 500 concurrent FTC and law enforcement users. The contractor shall permit law enforcement access to the data in two ways: (1) using a structured, intermediary function such as a query tool or parameterized report (constrained access); and (2) direct, unconstrained access to perform ad hoc reporting.

C.5.10.1.1 User Administration

C.5.10.1.1.1 FTC Staff

The FTC will provide the contractor with information regarding all FTC employees and contractors who need access to the system. All FTC employees and contractors assigned to the Bureau of Consumer Protection and regional offices shall be granted access to the system. The COTR or person designated by the COTR will authorize access for any other FTC users, and assign them a user role. (Through the discovery phase as discussed in Task Six, the contractor shall determine the FTC user groups.) The contractor shall provide the user with a user ID and password for access to the system.

C.5.10.1.1.2 Law Enforcement Users

The FTC will continue to approve Consumer Sentinel Network member agencies. The contractor shall develop and provide an online application for law enforcement users of Consumer Sentinel Network member agencies. (The current Consumer Sentinel Network User Application is CIS TE 1. This application is meant as an example only, and the requirements for the online application shall be discussed in the discovery phase.) The

contractor shall suggest methods to reduce or eliminate members of the public being able to access the law enforcement user application. The contractor also shall propose a method(s) for the FTC to verify the identity of law enforcer applicants.

The applications shall be made available online to the FTC to approve and assign the law enforcer to a user group, or reject. If approved, the contractor shall provide the user with a user ID and password for access to the system.

C.5.10.1.1.3 Data Receivers (Bulk Data Exports)

Certain data receivers will have access to a secure website to download bulk data files. The FTC will approve each data receiver organization (unless it is already an approved law enforcement agency). The COTR or person designated by the COTR will authorize access for users within data receiver organizations. The contractor shall provide each user with a user ID and password for access to the system. Data receiver users will have access only to the secure export website.

C.5.10.1.1.4 Access rights

Several groups shall be defined with specific access rights and the FTC and authorized external users shall be assigned to those groups. Users in a specific group will have access only to those parts and functions of the system and data that are identified for that group with privileges that were granted to that group.

C.5.10.1.1.5 Unlock Accounts

The system shall lock user accounts in accordance with the section on Physical and Information Security (C.1.12). The contractor shall work with the FTC to develop a policy regarding unlocking accounts, including verification that there is not a threat to system security and integrity. The contractor shall implement the policy and, for all accounts meeting the stated guidelines, unlock user accounts.

C.5.10.1.2 Integrate Current FTC and Law Enforcement Users

The contractor shall transfer and load all existing FTC and law enforcement user accounts into the system. The transfer shall maintain the integrity of the data – no data may be lost, altered or added. However, the contractor may work with the FTC to correct data discrepancies and suggest other methods for organizing the data (e.g., modifying or eliminating the "organization codes" for each agency and listing only by name, in alpha/numerical order).

C.5.10.1.3 Website Landing Pages

Upon successful authentication, all FTC and law enforcement users shall be directed to landing pages corresponding to their user groups. In the least, the landing page shall provide a summary of the user's alerts, scheduled searches, and saved searches (see Sub Task 2.2).

The user should be able to customize the landing page, within certain administrator defined parameters.

C.5.10.2 Sub Task 2.2: Provide Law Enforcement Constrained Access to Retrieve Data

The system shall allow law enforcement users to query and view data. The system shall provide a query interface that requires minimal skill in using a search engine. The query functionality shall be used to support record updates and data extraction. The FTC users may have more search fields than law enforcement users.

Queries may require searches and retrieval of both encrypted and unencrypted data. The contractor shall ensure that search and retrieval of encrypted data does not impact performance.

C.5.10.2.1 Data Sources

The system shall allow users to choose from one or more data sets as permitted by privileges assigned to their respective user groups. The data sets are: CIS, IDT, National Tape Library (NTL), DNC complaints, DNC consumer and telemarketer registry records, econsumer, and Military Sentinel.

C.5.10.2.2 Provide Access to DNC Registry Data

DNC consumer and telemarketer registry data is housed in the DNC contractor's database. The FTC and certain law enforcement users shall be able to query and obtain appropriate registry information. Although the registry information is housed in the DNC contractor's database, the user search experience shall be transparent and seamless, completely conducted through the system query interface. Thus, using a web service, the contractor shall develop and provide a secure method for authorized users to access and query the DNC registries, or the contractor may integrate the DNC registries with the system, provided that it also meets with the same security requirements.

C.5.10.2.3 Query Attributes

The system shall provide:

- field-level search functionality (all data (text or values) fields are searchable);
- Boolean and related search operators within fields ("and", "or", "not", "greater than", "less than", "equal", and use of parentheses or quotes to group words);
- Boolean operators "and" and "or" between fields;
- for searches by ranges of values;
- proximity searches (e.g., operators like "near", "within X" (within X number of words, sentences or paragraphs), "before", and "after");

- use of a wildcard character (e.g., for truncation and multi-character wildcard for finding alternative spellings);

- an option to search for records flagged as internet related;

- an option to select one or more suspects from a list of values;

- an option to save and load a pre-defined query; and

- a search within a search result set.

C.5.10.2.4 "Quick" Search

The system shall provide users with a "quick" search option which will be executed against a select set of data fields (e.g., suspect name, suspect address, etc.) and record attributes (e.g., identity theft complaints). The data fields and record attributes will be determined by the FTC in the discovery phase.

C.5.10.2.5 Scheduled Searches

The system shall provide an option to set an automated search to run for a user-defined frequency (daily, weekly or monthly) and deliver a message via email when there are results of the search. The scheduled search function shall have the following features:

- Users can set the duration for the scheduled search to run (within a maximum duration set by a business rule);

- Generate an expiration warning via email and offer an extension of user-defined amount of time (within maximum duration);

- Prompt user with an option to create an alert (see C.5.10.2.12) when saving a scheduled search;

- Users have the option to designate if they want to overwrite the previous results of the scheduled search each time the search is run, or maintain the results of all previous instances of the scheduled search. The default setting is overwrite the results with each new result set; and

- The notification email shall contain a link to the system page on which the user can view the results (after user authentication).

C.5.10.2.6 Query Results – Summary View

The system shall display query results in a column and row style summary of records displaying data from certain fields. The data views shall conform to the following:

- Sort summary search results by column;

- Display search criteria;
- Users can choose the columnar order in which the fields are displayed;
- Users should be able to set preference for columns and their order in their user profile;
- For quick search, callout the search term(s) in the results; and
- The summary view shall be in a printer-friendly format.

C.5.10.2.7 Query Results – Detailed Record View

The system shall allow users to drill down from the summary results to see a detailed record view. The user will be able to print a printer friendly formatted record of the detailed record view. The system also shall provide the user the option to define fields that should be redacted in this view and insert user-defined appropriate text instead (e.g., user chooses to redact consumer name field on all detailed records and display "redacted" in that field).

C.5.10.2.8 Save Query Results

The system shall provide users with the option to save the query results on the system (NOT saved locally). The saved search results shall be retrievable, and appear as they were returned on the day and time the search ran. This feature shall comply with the requirements stated in OMB Memorandum M-06-16 (e.g., deleted after 90 days, encrypted, etc.).

C.5.10.2.9 Improvement of Data Quality for Extraction

To improve data retrieval, the contractor shall develop and provide for a mechanism to logically link all permutations of a suspect name to provide comprehensive and accurate search results. The mechanism shall account for, among other things, proper name variations, misspellings, and commonly used name and abbreviation variations. Likewise, data retrieval should account for address discrepancies (USPS compliant address hygiene software can be used for this). Note that the FTC's policy is that the consumer data, as submitted, cannot be altered.

The contractor shall propose other automated methods to find commonalities, patterns and relationships among records to provide comprehensive and accurate search results. For example, the system may provide the user the option to return results corresponding to matching underlying suspect data (e.g., if one complaint has suspect name X and suspect phone number 123-555-1212, and another complaint has suspect name UNKNOWN and suspect phone number 123-555-1212, the second complaint would be associated with suspect name X and returned in a search for suspect name X).

C.5.10.2.10 Audit and Logging

The system shall audit and log all queries. The information that shall be audited and logged includes, at a minimum: user ID, date and time of the search, the search terms, and reference numbers of all extracted records containing sensitive information. The contractor shall maintain the logs indefinitely, unless otherwise directed by the FTC. The contractor shall provide the FTC access to the audit logs, and provide the capacity to query, sort, filter, view and print the logs.

C.5.10.2.11 Data Extraction (Following Query)

The system shall provide a download option to save the detailed records in the following formats: CSV, PDF, TXT, XLS and XML. The system shall allow the user to select the fields to download (within a set of fields defined by an administrator). Access to the download feature shall be limited by user role. The user shall be able to indicate that certain downloaded fields are redacted, and have the ability to assign what is to be displayed instead of the value. This feature shall comply with the requirements stated in OMB Memorandum M-06-16.

C.5.10.2.12 Provide "Alert" Functionality

Users shall have the capability to "alert" other users as to their interest in a particular target or attributes of a target (e.g., name, phone number, address, URL, etc.). When a query runs, the query terms and results are compared to all active alert data. If there is a match, the alert information is returned along with the search results in the summary view. Alerts are NOT linked to a particular record.

C.5.10.2.12.1 Ownership of Alerts

In creating alerts, users can delegate ownership of an alert (e.g., have a "created for" field) to another authorized user for the purpose of modifying or deleting the alert. Only alert owners may modify or delete alerts.

C.5.10.2.12.2 Search Alerts

The system shall provide an option to search for alerts. When searching alerts, the system shall allow a user to enter a search string and search all alert criteria.

C.5.10.2.12.3 Alert Expiration

The system shall provide an option to select an expiration date for the alert. The default expiration date shall be one year. The maximum duration for an alert shall be set by an administrator. The system shall send an email to the alert owner(s) with an expiration warning.

C.5.10.2.13 Provide Parameterized Reports

The contractor shall develop and provide a parameterized report ("Top Violator" report) that provides a list of those suspects with the most complaints (along with complaint

count). The report shall be based on the data set(s) as determined by the user's group. The possible data sets are: CIS, DNC and econsumer. Users shall be able to build the report using the following criteria (not all criteria are applicable depending on the data set): number of suspects (1 – 100); country (can select multiple values); date range (default to six months); state/province (can select multiple values or all); product/service code or DNC law violations (can select multiple values or all); for DNC, count by suspect name or subject phone number (integrate, if possible); choice between consumer state/province/country or suspect state/province/country, and internet-related check box. The system shall use the mechanism developed to logically link all permutations of a suspect name in order to provide comprehensive and accurate reporting results. The report results shall contain the report criteria and a table showing the suspect names with corresponding complaint count, in decreasing order of complaints. Each suspect name in the report results shall be a clickable link that will call up all complaints underlying the reported number (in the search results summary view).

C.5.10.2.14 Training Environment

The contractor shall develop and provide a web based training environment that replicates all system functions in the end user experience. The training database shall contain non-production ("dummy") data. The training environment shall be capable of handling up to 200 concurrent users. The FTC may use this training environment to demonstrate the system to persons and organizations that are not eligible to access the system.

C.5.10.3 Sub Task 2.3: Provide Direct Access to the Database for Reporting Tools

The contractor shall provide secure, direct, and unconstrained access to the consumer data to permit law enforcement to perform unstructured, ad hoc reporting. This access currently is limited to certain FTC personnel, but may be expanded to other FTC personnel and external law enforcers in the future. This access shall be accomplished without the need for an intermediary function, and a desktop, server-based or web based industry standard data reporting and analysis tool may be utilized. Currently, the FTC uses Business Objects as its reporting tool.

C.5.10.4 Sub Task 2.4: Bulk Data Exports

The contractor shall develop and provide a system that will download batch files. Bulk exports may be regularly scheduled or needed on an ad hoc basis. Exports shall be in either text - comma delimited or XML formats. The FTC will identify the parameters, fields, and, if applicable, format (e.g., Global Justice XML Data Model) for the export. All data in exports shall be encrypted (see section C.1.12 – Physical and Information Security).

C.5.10.4.1 Methods of Data Transfer

The contractor shall develop and provide the capability to transfer export files via web services. Alternatively, files may be transferred using a CD, DVD or as an email attachment.

The contractor shall develop and provide a secure website that will permit data receivers to download their data export files. The contractor shall take into account that the speed of contributors' connections to the internet will vary. The website shall be password protected and accessible only by data receivers approved by FTC. The website can be the same one that law enforcement uses to access the Consumer Sentinel Network (https://cs.sentinel.gov) or the same one used by data contributors (see Sub Task 1.4).

C.5.10.4.2 Redacted Fields in Data Export

The system shall have the capability to insert user-defined text for certain downloaded fields that need to be redacted (e.g., consumer names are not downloaded; instead, "consumer name redacted" appears in that field for each record).

C.5.10.4.3 Retention of Data

The contractor shall maintain duplicates of all export files. The duplicate export files shall be retained indefinitely, unless otherwise directed by the FTC. The duplicate export files shall be provided to the COTR or person designated by the COTR upon request.

C.5.10.5 Sub Task 2.5: Securely Exchange Data with Law Enforcement Networks

The FTC's IDT Uniform Law Enforcement Complaint/Report (described in C.1.2.4.3.2) requires that the contractor develop and provide a system that is capable of establishing secure XML data transfers with certain national and regional law enforcement networks to exchange, in real-time and using web services, data relating to identity theft affidavits.

This sub task shall be priced separately.

C.5.10.6 Sub Task 2.6: Additional Web Pages for Reference Materials

The system shall provide the following web pages for text and reference content: Library, Reports, Contacts, Orders, and National Tape Library. Prior to implementation of the system, other web pages may be added based on the requirements analysis. Except for the Contacts page, the FTC will provide content for each of these pages. These pages shall be capable of maintaining files in various formats (e.g., PDF, HTM, MS Word, WordPerfect, PowerPoint). The FTC will be able to request changes to these web pages monthly. In addition, the FTC will be able to request three emergency releases to these pages per quarter.

The contractor shall provide the content for the Contacts page based on all system user profiles. Users will be able to search based on the following criteria, at a minimum: last name, first name, city, state/province, country and organization name.

In addition, the contractor shall provide a manner for law enforcement users to access a complaint entry web page hosted by the contact center contractor. Access to the complaint entry page shall be transparent and seamless from the system developed under this task, and the user experience shall be completely transparent and seamless. The contractor shall work with the contact center contractor to develop a secure method to provide this access and transfer information.

After contract award, the FTC may request quarterly additional content web pages.

C.5.10.6.1 Content Management

The contractor shall provide the COTR or person designated by the COTR with privileges to manage content on the system. Alternatively, the COTR or person designated by the COTR may direct the contractor to add, modify or delete content on the system. If so directed, the contractor shall make the content changes accurately and completely and within two business days.

C.5.10.7 Sub Task 2.7: Customer Support for FTC, Law Enforcement and Data Receivers

The contractor shall provide customer support through: (1) an online tutorial for authorized users; (2) an online help system; and (3) receipt and resolution of user problems.

C.5.10.7.1 Tutorial

Upon accessing the system for the first time, authorized users shall be provided the option of using a tutorial about: various system functions available to the user (based on user group), the type(s) of data in the system, and protection of the confidential data. The tutorial shall be tailored to particular user groups. The contractor shall create the tutorial with input from the FTC. The tutorial shall be available to users at any time after their initial use of the system. The contractor need not prepare a tutorial for consumers.

C.5.10.7.2 Online help

The system shall provide information to support user real-time activities. The online help shall be context sensitive at the screen level. The system shall open the online help in a manner to permit users to view the appropriate function simultaneously.

C.5.10.7.3 Requests for Customer Service

The contractor shall ensure that it resolves any problems users experience in accessing or using the system.

C.5.10.7.3.1 Channels of Communication

The contractor shall receive requests for customer service via three channels of communication: telephone messages, email, and problem reports generated from within the system (e.g., "Contact Customer Service" link). The contractor shall respond to requests for customer service via telephone or email. When users call the contractor, they will hear a greeting and a call tree providing support options, including answers to frequently asked questions about access or use of the system. Users shall be given the option to leave a message and the option to be contacted via telephone or email. The contractor shall respond to telephone messages and email contacts within four hours inside normal business hours.

The contractor may combine the telephone customer service with the call center lines.

C.5.10.7.3.2 Escalation of Requests

All requests from authorized users that do not concern accessing or using the system (e.g., law enforcement eligibility for Consumer Sentinel Network membership, requests for FTC staff to attend events, data contributor questions about confidentiality of submitted data, etc.) shall be referred to the COTR or person designated by the COTR for appropriate action the same day as receipt.

C.5.10.7.3.3 Records of Requests for Assistance

The contractor shall maintain, for a period of two years from the date created, a record of all such requests for assistance. The record shall contain, at a minimum: the user's name, date and time received, phone or email contact, description of the problem, status, response provided by the contractor, date and time of the response(s), date of resolution, length of time to respond initially, and length of time to resolve.

C.5.10.7.3.4 2005 Data re Requests for Customer Service

In 2005, the FTC received about 1,800 calls and about 850 emails from external law enforcement users regarding problems experienced in accessing or using Consumer Sentinel. In addition, the FTC Help Desk had about 200 contacts from internal users about CIS. (Note that at this time, only FTC staff and law enforcement users have access to Consumer Sentinel.) Due to the fact that this will be a newly redesigned system, and it will be available to authorized data contributors and receivers in addition to FTC staff and authorized law enforcers, the FTC cannot accurately predict the number of customer service requests the contractor will receive.

C.5.11 Task Three: Reports

The contractor shall provide periodic reports via a secure website for remote access, download and printing by the COTR or any person designated by the COTR. The COTR shall be able to manipulate, sort and filter the reports. The reports shall be downloadable to Excel. The contractor shall make the reports available for remote access for two (2) years after the date created.

Daily reports are due the following business day by 8:00 a.m. Eastern time. Weekly reports are due within one business day after the conclusion of each week. Monthly reports are due within three business days after the conclusion of each month. Quarterly reports are due within five business days after the conclusion of each quarter. Annual reports are due within five business days after the conclusion of the calendar year.

At a minimum, the reports must include:

REPORT	ATTRIBUTES	FREQUENCY
Imported records	1. Contributor 2. Number of raw records 3. Number of records imported into database 4. Number of records that failed to be loaded into database and reason(s) for failure 5. Cumulative total of contributor's records loaded into database YTD	Next business day after each import Monthly and annual summaries
Imported records awaiting QA	1. Contributor 2. Date data received 3. Number of raw records	Next business day after each upload
Total records loaded into the database	Broken down by contributing organization	Weekly and quarterly
Exports	1. Data receiver 2. Number of records by source (e.g., IDT, general, etc.)	Next business day after each export Monthly and annual summaries
Authorized user accounts created/modified/deactivated	1. Broken down by user (alpha) and by organization 2. Indicate create, modify or deactivate (if deactivate, why) 3. Total number of each	Daily
Locked user accounts		Daily
User access/hits on web pages	Broken down by user (alpha), by organization and web pages visited; be able to sort by user, organization, and web pages.	Weekly and quarterly

REPORT	ATTRIBUTES	FREQUENCY
Query performance (constrained access – Sub Task 2.2)	For any query results that were not returned within the performance standard (5 seconds or less): 1. User ID 2. Query criteria 3. Amount of time for query to run 4. Reason(s) for query to not run within the performance standard 5. Total number of queries not returned within performance standard and as a fraction (percentage) of the total number of constrained access queries.	Weekly and monthly views
Number of queries and system usage	Broken down by constrained vs. unconstrained queries; users; etc.	Weekly
Requests for customer service	Phone v. email, nature of the problem, status, time to respond.	Weekly

The FTC may update the format and attributes of the reports quarterly.

C.5.11.1 Other Reports

The contractor shall provide, at the COTR's request, periodic reports about performance of the requirements of this contract, including statistical information. The FTC annually may request up to six reports on an ad hoc basis, at no additional cost.

C.6 PROJECT PHASES AND INTERIM WORK PRODUCTS

The contractor shall develop and provide the system according to the following phases. Progressing to the next phase is contingent upon the factors (including interim work products) outlined below.

C.6.1 Project Planning Phase

Two weeks after contract award, the contractor shall submit a project plan describing project execution and control. The project plan shall contain, at a minimum: roster of team members, along with roles and responsibilities; major milestones with descriptions

and dates (project schedule); key risks; and organizational strategy and management strategy. It is expected that this document will change over the course of performance.

C.6.2 Discovery Phase

The contractor shall undertake a study of the business processes and functions of the stakeholders who will use the system. The contractor shall use this study to analyze and further refine the requirements of this contract and build a business architecture about the system users and how they will use the system. Upon completion of this phase, the contractor shall submit a detailed requirements analysis and standards report. This phase will be considered complete upon approval of the requirements and standards report by the FTC.

C.6.3 Design Phase

Based upon the requirements analysis and standards report, and per section C.5.3, the contractor shall submit all websites, online forms, function screens, tutorial tools and help systems to the FTC for review. In addition, the contractor shall provide the FTC with wireframes of web pages and interfaces. This phase will be considered complete upon the FTC's approval of the design, content and functionality of the aforementioned items and wireframes.

C.6.4 Test Phase

The contractor shall provide a final version of the system for testing at least 30 days prior to deploying the system. All data used in this phase shall be CIS data. Data will be entered, queries and reports will be run, and security features shall be challenged. Testing shall occur in an environment which simulates the production environment. The contractor shall consider using releases (i.e., alpha, beta, etc.) to reflect changes made to correct defects and in response to feedback from testers. During this phase, the contractor shall develop an implementation plan. This phase will be considered complete upon remedy of all significant defects and delivery of an implementation plan, and acceptance of both by the FTC.

C.6.5 Implementation Phase

The contractor shall deploy the system and perform the requirements as set forth in the specific tasks section.