



**PRIVACY IMPACT ASSESSMENT (PIA) FOR:**

**Consumer Response Systems and Services  
(CRSS)**

**June 2008**

The Federal Trade Commission's (FTC) Bureau of Consumer Protection (BCP) protects consumers from a variety of fraudulent, deceptive, and unfair practices in the marketplace, including identity theft, telemarketing fraud, Internet fraud, and consumer credit issues. To further its consumer protection mission, the FTC brings civil and administrative law enforcement actions to enforce its laws and provides consumer and business education to enable the public to avoid common harms. The FTC works to ensure that consumers have accurate information for purchasing decisions, and confidence in the traditional and electronic marketplaces.

BCP's consumer protection-related activities include consumer complaint collection and analysis, individual company and industry-wide investigations, administrative and federal court litigation, rulemaking proceedings, consumer and business education, and the operation of consumer protection programs.

One focus of these activities is the enforcement of the Telemarketing Sales Rule (TSR) and do not call regulations (16 C.F.R. Part 310). BCP uses the National Do Not Call Registry<sup>®</sup> (DNC) to protect consumers from unwanted telemarketing sales calls and to make complaints about calls they receive; to assist telemarketers in complying with regulations; and assist law enforcement investigations of violations.

In addition, BCP uses the Consumer Response Center (CRC) to allow consumers to report instances of identity theft and other consumer protection complaints; to guide and educate consumers; and to assist law enforcement investigations of alleged violations. The CRC acts as both an information collection and dissemination point to assist in mission achievement.

Information received by the FTC is stored in a database called the Consumer Information System (CIS). A large portion of this information is made available to thousands of civil and criminal law enforcement members in the United States and abroad through a secure Internet website called the Consumer Sentinel Network (CSN). CSN thus makes the complaint filing and collection process more efficient for both consumers and law enforcement; consumers file one complaint that can be accessed by numerous agencies, each of which may have jurisdiction and the ability to assist the consumer or prosecute the alleged violation. The CSN is used to make available, analyze and extract data, and to provide a host of other investigatory tools to members.

BCP's DNC, CIS and CRC programs together with CSN are collectively referred to as Consumer Response Systems and Services (CRSS). The FTC has contracted with Lockheed Martin Business Process Solutions (LMBPS) to implement, maintain, and operate CRSS, which is targeted to go live in June 2008. BCP has conducted this Privacy Impact Assessment on CRSS as part of the Certification and Accreditation process for major information technology systems.

## **1.0 SYSTEM OVERVIEW**

CRSS is a powerful consumer protection data source, much of which is available to the federal, state, local, and international law enforcement community. CRSS data is also used to identify and track trends and potential problems affecting the marketplace. CRSS contains data collected by the FTC as well as data collected by other entities and forwarded to the FTC. External contributors include a broad array of public and private domestic and foreign organizations.

CRSS uses several applications or components to collect and share consumer data as described below. CRSS related data is owned by BCP's Division of Planning and Information.

### **1.1 Consumer Response Center (CRC)**

The Consumer Response Center gathers, processes and updates consumer information via call center services and Internet-based complaint forms. Users access a multi-channel bilingual (English and Spanish) contact center to file complaints, report instances of identity theft, and request or receive consumer education materials. Consumers interact with the CRC via secure Internet complaint forms found on [FTC.gov](http://FTC.gov), [Consumer.gov/Sentinel](http://Consumer.gov/Sentinel), [Consumer.gov/IDTheft](http://Consumer.gov/IDTheft), [FTC.gov/idtheft](http://FTC.gov/idtheft), [Consumer.gov/Military](http://Consumer.gov/Military), [eConsumer.gov](http://eConsumer.gov), and [Donotcall.gov](http://Donotcall.gov), toll-free telephone numbers (1-877-FTC-HELP and 1-877-ID-THEFT), and postal mail. Toll-free services include:

- Interactive Voice Response (IVR)
- Automated Voice Response (AVR)
- TTY (for hearing impaired persons)
- Live telephone conversations with customer service representatives

With the launch of CRSS in June 2008, filing complaints online will become easier for consumers. They will now use the new Complaint Assistant Wizard to file complaints by answering a series of questions organized in a few simple steps. Hyperlinks to the new Complaint Assistant Wizard - <https://www.ftccomplaintassistant.gov/> - will be available through [FTC.gov](http://FTC.gov) and the various CRC online complaint forms.

The CRC currently handles about 2 million consumer interactions per year - about 50% of these interactions are automated. Consumer complaint data received through the CRC is entered into the CIS database.

### **1.2 National Do Not Call Registry® (DNC)**

DNC consists of four major functions: consumer registration, telemarketer access, law enforcement access, and consumer complaints. The consumer registration function allows consumers to register their telephone numbers and to verify whether their phone numbers are on the registry. Consumers carry out these activities through the secure Internet site at

[www.donotcall.gov](http://www.donotcall.gov) or via nationwide toll-free telephone numbers (1-888-382-1222 or TTY 1-866-290-4236). Consumers may also delete their telephone numbers by using the toll-free system, if they are calling from the phone that is registered. Users of the consumer Internet site or toll-free telephone number may interact with DNC in English or Spanish. In addition, the telephone system supports hearing impaired persons through a toll-free number for teletypewriter (TTY) access.

Telemarketers may access DNC through the Internet site [telemarketing.donotcall.gov](http://telemarketing.donotcall.gov). New telemarketers create a profile and receive an organization ID and password. They then subscribe to area codes they need and, if required, pay for their subscription. Upon successful completion of that step, they download registered consumer telephone numbers to ensure that they do not call those numbers. Telemarketers originally were required to download and scrub their lists every 90 days; in 2005, this was shortened to 31 days. Upon creating their profiles and each and every time telemarketers download from the registry, they must certify that their organization will comply with the DNC requirements. In addition, telemarketers may access an online helpdesk system to obtain assistance with technical questions and issues.

CSN law enforcement members in the United States, Canada, and Australia may access the DNC system to support investigations of violations of the Telemarketing Sales Rule. These Sentinel members can access information about the registration, verification, and deletion transactions for individual consumer telephone numbers. They may also gather information about telemarketer enrollment profiles, clients, subscriptions, and downloads.

Consumers may file complaints about alleged violations of the do not call rules. Like the registration function, consumers may access the complaint function either over the Internet or by telephone. Consumer complaint data received through DNC is captured by the CRC, stored in the CIS database, and made available on the CSN.

### **1.3 Consumer Sentinel® Network (CSN) and the Consumer Information System (CIS)**

CSN includes the following series of interconnected websites:

- Consumer Sentinel® - general fraud, identity theft (IDT), DNC, and other complaints
- Consumer Planet Sentinel - cross-border e-commerce complaints
- Military Sentinel - fraud and identity theft complaints from military personnel

Consumer Sentinel is the website through which local, state and federal law enforcement agencies in the United States, Canada, and Australia access consumer fraud, identity theft, and DNC complaints collected by the CRC and stored within the CIS database. Included within Consumer Sentinel is the IDT Data Clearinghouse which is the nation's repository of identity theft complaints. These complaints are made available through CSN.

The Consumer Planet Sentinel (CPS) website is also housed within CSN. CPS membership is open to government agencies in those countries that belong to the International Consumer Protection and Enforcement Network (ICPEN). CPS is part of [econsumer.gov](http://econsumer.gov) ([www.econsumer.gov](http://www.econsumer.gov)), an international project focusing on cross-border e-commerce fraud. The [econsumer.gov](http://econsumer.gov) site offers cross-border consumer protection information and an online complaint form. All information on [econsumer.gov](http://econsumer.gov), including the complaint form, is available in English, Spanish, French, and German. Additionally, all information other than the complaint form is available in Polish, Japanese, and Korean. Cross-border e-commerce complaints received from consumers through the [econsumer.gov](http://econsumer.gov) complaint form are entered into CIS. CPS users can access only those complaints received through [econsumer.gov](http://econsumer.gov).

Military Sentinel 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 consists of a public Internet site and a restricted Internet site accessed through the CSN. The Military Sentinel public site also provides a gateway to consumer education materials covering a wide range of consumer protection issues, including issues that are directed to members of the military. The complaint forms on the Military Sentinel public site allow consumers to identify their service branch, posting, and pay grade. Complaints entered into Military Sentinel go directly into CIS, and are accessible by users through the CSN. Consumer complaints submitted through Military Sentinel's public Internet site are also accessible by DOD consumer education staffers through the Military Sentinel restricted Internet site. These DOD consumer education staffers may only access complaints entered into Military Sentinel, and do not have access to any other portion of the CSN network. In addition, DOD consumer education staffers are not provided access to consumers' personally identifying information (e.g., name, address, telephone number).

Authorized users access the CSN through a secure, password-protected Internet site which uses two factor authentication. They then can search complaints in the CIS database. CSN users' access to the various subsets of CIS data is based on the organization to which they belong. For example, currently, only US law enforcers may request access to all complaints in both Consumer Sentinel and the IDT Data Clearinghouse. Canadian law enforcers may request access to Consumer Sentinel information, as well as all IDT complaints submitted by Canadian data contributors, and IDT complaints submitted by US data contributors that have an entry date after July 1, 2003.

Authorized CSN users may search CIS using criteria which include company or suspect name, address, telephone number, consumer location, or type of scam or identity theft. As of March 1, 2008, the CSN served over 1,700 law enforcement agencies across the world that have signed appropriate confidentiality agreements restricting their use and disclosure of CIS data to law enforcement purposes.

With the launch of CRSS in June 2008, a new and improved CSN Internet site with expanded capabilities, faster searches, stronger security, and a fresh look will be launched. The new CSN will be an even more effective tool for immediate and secure access to consumer complaints about identity theft, Internet fraud, telemarketing, and scams. With the new CSN, authorized law enforcement users will be able to:

- Find complaints faster and more easily
- Store search results in 100 MB of online storage space on Consumer Sentinel
- Search within searches
- Gather related complaints using keywords in the search results
- Extract a limited number of complaints from the system for use in their investigations

The new CSN will be accessible via the following secure Internet site addresses:

- [www.consumersentinel.gov](http://www.consumersentinel.gov)
- [www.consumersentinelnetwork.gov](http://www.consumersentinelnetwork.gov)
- [www.sentinel.gov](http://www.sentinel.gov)

## **2.0 Information Collected and Stored Within CRSS**

### **2.1 What information is collected, used, disseminated, or maintained by CRSS?**

The CRSS CRC components collect and maintain personal information that consumers voluntarily submit when they contact the FTC to file a complaint or to request information. The CRC collects such information directly from consumers, or from their guardians or others acting on their behalf who may provide the information by using the CRC's online consumer complaint forms, or by calling or writing to the CRC. The personal information may include:

- First and last name
- Street address, city, state, country and postal code
- E-mail address
- Date of birth or age range, only for complaints and IDT requests for information
- Contact telephone number(s)
- Social Security Number (SSN), only if applicable
- Relationship to suspect, only for identity theft complaints
- Account number, only for identity theft complaints
- Driver's license number, only for identity theft complaints
- Free-form description of the consumer's issue(s)

For two categories of complaints, identity theft-related complaints and complaints related to the accuracy of consumer credit reports, CRSS allows the consumer to provide a SSN. Consumers

submitting complaints to the Identity Theft Data Clearinghouse are asked to provide their SSN in order to assist law enforcement with identity theft investigations. Consumers submitting complaints about the accuracy of consumer credit reports are asked to provide their SSNs to enable the consumer reporting agency (CRA) to accurately and efficiently match the consumer complaint to the CRA's files, pursuant to a statutory complaint sharing and resolution initiative (see section 3.3). CRSS encrypts the SSN, and the number is not displayed when members search the system. CRSS also collects and maintains the subject matter of consumers' complaints and information regarding the companies, entities, or individuals about which the consumer is complaining. If the complaint is reported by someone else on behalf of the consumer, then name, address, and contact information of the person reporting the complaint is also captured along with the affected consumer's information, and both are stored in CRSS.

When a consumer complains about an individual, as opposed to a company or other entity, the CRC may collect the following personal information about the individual against whom the consumer is complaining:

- First and last name
- Middle name and suffix, only for identity theft complaints
- Street address, city, state, country and postal code
- E-mail address
- Telephone number(s)
- Date of birth, only for identity theft complaints
- SSN, only for identity theft complaints
- Individual's relationship to consumer, only for identity theft complaints
- Method individual used to obtain the complainant's personal information without authorization, only for identity theft complaints

In addition to the standard information collected on the CRC's other online complaint forms, the complaint forms on Military Sentinel allow consumers to identify their service branch, posting, and pay grade.

For system auditing purposes, CRSS also collects and stores the following user responses, computer system and network related information along with the consumer complaints:

- Answers or responses provided by consumers to the questions presented by the online Complaint Assistant Wizard or the IVR/AVR while gathering their complaints
- Date and time when the consumer's complaint is submitted or updated

- Name of the domain and host from which the consumer gained access to the online complaint forms
- Internet address of the site from which the user linked directly to the online complaint forms
- Internet protocol (IP) address of the computer the consumer was using when submitting a complaint online
- User's Internet browser software information
- User's computer Operating System information

CRSS also includes consumer complaint data collected and forwarded to the FTC by external data contributors. External data contributors include a broad array of public and private domestic and foreign law enforcement, consumer protection, and other organizations. The consumer complaint data collected from external data contributors includes the same types of data collected by the CRC.

DNC collects and maintains information that consumers voluntarily submit either via the Internet site or by calling the DNC's toll-free telephone numbers. For registrations, verifications, and deletions completed over the telephone, the only information provided by consumers is their telephone number. Consumers registering via the DNC Web site must also provide an e-mail address, which is used as part of an online confirmation process that includes the delivery of an e-mail message and online confirmation transaction. Importantly, the DNC registry uses a secure hash algorithm to maintain the security of consumer e-mail address information. For consumers calling the DNC toll-free telephone numbers, access control is limited by requiring that they must call from the telephone that they wish to register, delete, or verify. The DNC only collects telephone numbers and the numbers are not associated with any other information, including e-mail addresses.

For DNC complaints, consumers must provide the telephone number that the telemarketer called, when the telemarketer called, and the name and/or the telephone number of the telemarketing company. Optionally, consumers may also provide their name and address. Future enhancements to the system will enable consumers to provide comments, as well. Consumers are cautioned not to provide personally identifiable information such as their SSNs.

When telemarketers enroll and create their profiles, they must provide the following information: their organization name and address; Employer Identification Number (EIN) or SSN in the case of a sole proprietorship; organization contact person; and the contact person's telephone number and e-mail address. If an entity is accessing the registry on behalf of a seller-client, the entity also will need to identify that client. Telemarketer payment information, including account

numbers, is handled by Pay.Gov, the federal government payment processor operated by the US Department of the Treasury, and is not shared with DNC. Telemarketers who submit requests to DNC's online Help Desk are explicitly cautioned not to provide their EIN, SSN, or account numbers when they make a Help Desk request.

When telemarketers download the list of telephone numbers from the DNC, the system keeps track of the area codes of the telephone numbers that are downloaded. For system auditing purposes, CRSS also collects and stores the following computer system and network related information:

- Date and time when the user gained access to CRSS
- Name of the domain and host from which the user gained access to CRSS
- Internet address of the site from which the user linked directly to the CRSS site
- Internet protocol (IP) address of the computer the user was using
- User's Internet browser software information
- User's computer Operating System information

Finally, law enforcement users requesting access to the CSN must go through a comprehensive and secure registration process and become approved and authorized members before being given access to the information available in the system. During the law enforcement organization registration process, we collect name, mailing address, email address and contact information associated with the organization requester, organization administrator, and the approving authority within the applying organization. In addition, we also gather the static IP address range that the organization's computers will use when accessing the Internet. During the individual law enforcement user registration process, we collect the law enforcer's name, work address, telephone number, and email address, as well as a copy of their government issued ID or badge.

In addition to law enforcement users, relevant sections of CSN may be accessed by approved data contributors to periodically upload and contribute bulk consumer complaint data to the FTC. These approved data contributors will only have access to those sections of CSN that enable submission of bulk complaint data, and will not have access to the complaint data maintained in the system. Name, mailing address, email address, and phone contact information of respective and approved data contributors is collected and stored in CRSS. Similar to data contributors, relevant sections of CSN may also be accessed by approved data receivers who may periodically login and download requested complaint data exported out of CRSS. Currently, these data receivers are limited to consumer reporting agencies (CRAs), which are provided certain data pursuant to a statutory mandate, and approved CSN law enforcement

members (see section 3.3 for a discussion of data sharing with CRAs). These approved data receivers will only have access to those sections of CSN that enable downloading of requested complaint data. Name, mailing address, email address, and phone contact information of prospective and approved data receivers is collected and stored in CRSS.

Similar to CRC and DNC, CSN captures the following computer system and network related information for system auditing purposes:

- Date and time when the user gained access to CSN
- Name of the domain and host from which the user gained access to CSN
- Internet address of the site from which the user linked directly to the CSN site
- Internet protocol (IP) address of the computer the user was using to access CSN
- User's Internet browser software information
- User's computer Operating System information

## **2.2 What are the sources of the information in CRSS?**

Complaints maintained in CRSS are voluntarily submitted by consumers, or others acting on their behalf, to either the CRC or to our external data contributors. The major external data contributors to CRSS currently include the following:

- The Internet Crime Complaint Center (IC3)
- Participating Better Business Bureaus (BBBs)
- Phonebusters
- The US Postal Inspection Service (USPIS)
- The National Fraud Information Center (NFIC)
- The Identity Theft Assistance Center (ITAC)

NOTE: a complete list of data contributors is available in the FTC's annual Consumer Fraud and Identity Theft Complaint Data report. A copy of the 2007 report can be found at <http://www.consumer.gov/sentinel/pubs/top10fraud2007.pdf>.

CRSS does not receive data from commercial data brokers or information resellers.

In addition, consumers who wish not to receive telemarketing calls can register their telephone numbers on the DNC, either online via the DNC Web site, or by calling the toll free phone numbers. Telemarketer information gathered by DNC is provided by telemarketers and sellers. Law enforcement organization and user information for access to the CSN is provided directly by the law enforcement member and their respective organization.

### **2.3 Why is the information being collected, used, disseminated, or maintained?**

The FTC collects and maintains consumer complaints to further its consumer protection mission. By collecting, maintaining, and analyzing this data, the FTC is better able to target law enforcement action, provide consumer and business education to protect the public, and identify trends in consumer fraud and law violations.

As explained above (see section 2.1), the FTC collects SSNs for two categories of complaints, identity theft complaints and complaints related to the accuracy of consumer credit reports. Consumers submitting complaints to the Identity Theft Data Clearinghouse are asked to provide their SSN and other sensitive PII (e.g. account numbers, driver's license number, etc.) in order to assist law enforcement with identity theft investigations. Consumers submitting complaints about the accuracy of their consumer credit reports are asked to provide their SSNs to enable the CRAs to accurately and efficiently match the consumer complaint to the CRA's files. CRSS encrypts the SSN, and the number is not displayed when members search the system.

The FTC collects and maintains consumer telephone numbers in DNC to make them available to telemarketers for the purpose of ensuring that telemarketers do not call the numbers on the registry. In addition, all registration, verification, and deletion transaction history for individual telephone numbers is maintained to assist law enforcement action.

All telemarketers' identifying information, including profile information, which includes EINs and SSNs, is maintained to assist law enforcement investigations. Law enforcement members of the CSN have access to this information.

The computer system and network related information collected by CRSS is used to determine the number of visitors to different sections of the respective Web sites including DNC, CRC, and CSN to help make the corresponding sites more useful, to help ensure the proper operation of these sites, and to help resolve Help Desk requests. CRSS collects consumers' IP address information to prevent abuse and to protect the integrity and security of the system. This information is not used to track or record information about individuals.

Consumers are instructed not to provide personal information such as SSNs, credit card numbers, bank account numbers, driver license numbers, health information, etc. in the comment portion of complaint forms, when filing a complaint online or calling the CRC. In addition, when a complaint is filed by a minor under the age of 13, any personally identifying information in that complaint will be deleted and purged. The FTC may periodically accept complaints about minors from law enforcement partners or other third parties, when such information is needed to effectuate law enforcement investigations, and when such information is gathered and shared in a manner that complies with applicable statutes and regulations (e.g. the Children's

Online Privacy Protection Act (COPPA)). In addition, the FTC will accept identity theft complaints filed by an adult on a minor's behalf. For DNC online registration, the online registration wizard only collects consumer telephone numbers and email addresses.

For complaints submitted via Military Sentinel, the FTC allows consumers to identify their service branch, posting, and pay grade. This information is collected to enable Military Sentinel users and DOD consumer education staffers to better investigate and follow-up on complaints submitted by consumers in the armed forces.

As mentioned above (see 2.1), the FTC also collects information from law enforcement users who request access to the CSN. This information includes contact information (e.g. name, address, etc.), as well as IP address information. The FTC collects and maintains this information to help ensure the security of the system. In addition, to foster law enforcement cooperation, contact information for CSN law enforcement users is made available to CSN members, and a list of all CSN member agencies is made available to the public.

#### **2.4 How is the information collected?**

The consumer complaint information gathered by the CRC is collected through the following channels:

- Interactive Voice Response (IVR) and Automated Voice Response (AVR) units collect data via interactive toll-free telephone sessions with consumers. Consumers may complete their transaction in the IVR/AVR or be passed to a customer service representative for further processing.
- Customer service representatives at the contact center enter or update complaints during live conversations with consumers. The customer service representatives use a complaint/identity theft entry/update interface that ensures the collection of required data elements.
- Complaints are entered directly by consumers via online complaint forms.
- Physical mail, received via US mail, is entered into the system by customer service representatives using the contact center complaints/identity theft interface. Physical mail is retained onsite at the contact center for a period of one year, after which it is shredded.

Consumers can access the online complaint forms directly from the FTC's primary Internet site at [www.ftc.gov](http://www.ftc.gov). General consumer and identity theft complaint forms are available in English and Spanish. Other public Internet sites through which the FTC's CRC collects online complaints that are entered into CIS include:

- The Consumer Sentinel public site ([www.consumer.gov/sentinel](http://www.consumer.gov/sentinel)) for general consumer complaints;
- The IDT site ([www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)) for identity theft complaints;
- The National Do Not Call Registry<sup>®</sup> site ([www.donotcall.gov](http://www.donotcall.gov)) for complaints related to violations of the Telemarketing Sales Rule and the Do Not Call Registry;
- The econsumer.gov site ([www.econsumer.gov](http://www.econsumer.gov)) for complaints relating to cross-border e-commerce fraud (which provides online complaint forms in English, Spanish, French, and German); and
- The Military Sentinel public site ([www.consumer.gov/military](http://www.consumer.gov/military)) for complaints from service members, their families, and DOD civilians.

These collections have been reviewed and approved by OMB (OMB Control No. 3084-0047) in accordance with the Paperwork Reduction Act.

With the launch of CRSS in June 2008, all of the above Web sites will link to the new Complaint Assistant Wizard to be made accessible at [www.ftccomplaintassistant.gov](http://www.ftccomplaintassistant.gov).

For complaint data contributed by external organizations, most of the contributors send batched data using CDs, DVDs, e-mail, or through a secured Web interface. The FTC retains 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 CRSS database. For data files received via e-mail or Web service, the FTC encrypts the original data. At the end of this retention period, the FTC purges the original files. If the files were transmitted via CD, DVD, or similar portable media, the media is destroyed in a manner that is consistent with OMB and NIST security standards.

DNC registration and complaint information is collected either through the toll-free telephone numbers or the Internet site ([www.donotcall.gov](http://www.donotcall.gov)). Telemarketer information is gathered through the telemarketer Internet site ([www.telemarketing.donotcall.gov](http://www.telemarketing.donotcall.gov)).

## **2.5 How will the information be checked for accuracy and timeliness?**

Consumer complaints collected by the CRC and DNC, or provided by data contributors, are not checked for accuracy or validity. This information is provided voluntarily by consumers and is made available for law enforcement use and investigation (also see 2.8, below). Telemarketer data submitted to DNC also is not checked for accuracy when it is submitted. However, telemarketers submitting that information must certify under penalty of perjury that the information they provide is true, correct, and complete. Information submitted by law enforcement organizations and their users who are requesting access to CSN is reviewed by the FTC and LMBPS before the application is approved and the user is granted access.

**2.6 Is CRSS using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?**

Yes, CRSS is using new technologies in ways that the FTC has not previously employed, and is combining these with existing technologies to enhance the security and privacy of the information housed within the system.

To protect individuals' privacy, encryption technology is used to ensure information confidentiality and integrity. All sensitive data are encrypted during transmission between the CRSS web portals and the end users or external systems using 128-bit Secure Socket Layer (SSL) encryption and Secure Hyper Text Transfer Protocol (HTTPS). Data downloaded or exported from CRSS are encrypted and password protected. In addition, all data stored by CRSS will be encrypted at rest using hardware encryption. Importantly, all encryption and data transport protocols will meet OMB and NIST standards.

In accordance with OMB and NIST standards, access to the CRSS CSN portal will be strictly controlled, and will utilize a minimum of two authentication factors. Authentication factors will include, unique user names, passwords, one-time passcodes generated by RSA SecureID tokens, approved IP address ranges, and such other factors as the FTC may determine are necessary to ensure the confidentiality and security of the system and its data.

All user access and operations are logged and logs are kept on a centralized logging server. The logs will be used to audit user access and produce relevant security reports. In addition, the CRSS application network perimeter is protected through advanced firewalls and Intrusion Detection Systems (IDS).

**2.7 What law or regulation permits the collection of this information?**

Several statutes authorize the FTC to collect and maintain consumer complaints. Section 6(a) of the FTC Act, 15 U.S.C. § 46(a), authorizes the Commission to compile information concerning and to investigate business practices in or affecting commerce, with certain exceptions. In addition, the Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 note, mandates the Commission's collection of IDT complaints, and the Fair and Accurate Credit Transactions Act of 2003, Pub L. 108-159, 117 Stat. 1952, requires the sharing of information with consumer reporting agencies.

Amendments to the Telemarketing Sales Rule (TSR), 16 C.F.R. Part 310, required the implementation of the National Do Not Call Registry<sup>®</sup> and collection of consumer telephone

numbers and DNC-related complaints. The TSR also requires telemarketers to access the National Do Not Call Registry<sup>®</sup>. Telemarketer SSN/EIN collection is mandatory under 31 U.S.C. § 7701.

## **2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?**

Considering the type of information collected and sources of collection, the following privacy risks were identified:

- Consumers might accidentally provide sensitive PII information in the complaint's Comments field that is not required by CRSS, which pose a risk of identity theft.
- Someone may try to pose as an authorized law enforcement user and try to register and obtain access to CSN, which can pose a security and privacy risk to the system.
- Data provided by consumers and/or data contributors might not be accurate, complete, or timely.
- Data provided by consumers and/or data contributors might be misused or improperly disclosed or accessed.

**NOTE: Privacy risks and mitigation are discussed in various sections throughout this document, including sections 2.8, 3.1, 3.2, 3.3, 4.1, 4.6, 5.5, and 7.3.**

To mitigate the risk of unnecessary PII being provided by consumers, the CRC uses the new Complaint Assistant Wizard which assists consumers in filing online complaints, and which only collects the information that is relevant to a given complaint. DNC online registration and complaint forms are designed in a way that consumers can only provide required information, reducing the risks of user accidentally providing PII information. In addition, consumers are reminded not to provide sensitive PII in the comments field.

To mitigate the risk of unauthorized access to the CSN, CSN employs a well defined and secure process to enable interested law enforcement organizations and their users to register and obtain access and thereby mitigate any associated security risks. This process requires users to enter a matching passcode that is specifically assigned to their law enforcement organization, submit valid and accurate information including email addresses that match their organization's email domain, and submit proper credentials, such as their badge, to verify that they indeed work for their respective organization.

As to the risk that data provided by consumers and data contributors might not be accurate, complete, or timely, it is important to note that CRSS purposefully accepts self-reported consumer complaint information, and makes the process of filing complaints as easy as possible for consumers. Importantly, the information provided by consumers is well suited to the

purposes for which it is collected - to support the FTC's law enforcement investigations and mission.

With respect to the use and disclosure of CRSS data, the FTC recognizes that there is a risk that consumers' information may be misused or disclosed for an unauthorized purpose. To mitigate the risk that this may be caused by a contractor, the FTC requires that all contractors involved with data collection and processing, as well as technical support of CRSS, submit to a rigorous security clearance process, sign a non-disclosure agreement, and agree to act in accordance with specified rules of behaviour.

To mitigate the risks associated with access by external law enforcement members, CRSS utilizes numerous procedural controls, which include a confidentiality and data security agreement. Each member agency and each user agrees, in writing, to maintain the confidentiality and security of CRSS data and only to use it for law enforcement purposes (see section 3.3 for a more detailed list of these controls). In addition to the confidentiality and data security agreement, the FTC periodically provides CRSS users with information on how CRSS data may be used and disclosed. If the FTC discloses CRSS data in another manner (e.g., in response to a FOIA request or to an entity that is a subject of a complaint), it redacts personal identifying information.

In addition, as discussed throughout this document, CRSS employs a significant number of layered technical controls to help prevent the misuse or improper disclosure or access of CRSS data.

### **3.0 Use and Access to Data in CRSS**

#### **3.1 How will information in CRSS be used?**

Both the FTC and external law enforcement members of the CSN use CRSS data to accomplish their consumer protection and criminal law enforcement missions. Specifically, CRSS data is used to identify potential targets for law enforcement actions. CRSS data also may be used as evidence in legal proceedings and may be filed in court. In addition, CRSS data may be used to help resolve consumer complaints, locate victims, respond to inquiries, provide consumer and business education, and identify trends. CRSS data also is used to assist with consumer redress, periodically review the effectiveness of the FTC's current consumer protection regulations, and develop consumer and business education programs and publications. Aggregate numbers compiled from CRSS data also help determine the effectiveness of the FTC's consumer protection program in accordance with the Government Performance & Results Act.

Telephone numbers included in DNC are shared with telemarketers to ensure that telemarketers do not call those numbers. Information provided by telemarketers to DNC is made available to both the FTC and our Sentinel members for law enforcement purposes. CRSS data is used in

accordance with the routine uses outlined in the FTC's Privacy Policy and Privacy Act System of Records Notices.

All uses of the CRSS data are both relevant and necessary to the purpose for which the data was collected. In addition, all CRSS users have a level of access determined by their need-to-know, with the lowest level of access needed to perform their work.

CRSS limits users' access to the features, functions and data for which they are authorized. For example, the contractors involved with data collection can only view the data which they enter or update, CPS users only can view data received through econsumer.gov, DOD consumer education staffers only can view data received through Military Sentinel, and data contributors only can access parts of the system that will allow them to contribute their data. Users cannot view Social Security Numbers. External users access the CRSS applications through 128-bit SSL encryption and strong two factor authentication. FTC also maintains audit logs of each user's activity in CRSS.

### **3.2 Which internal entities will have access to the information?**

Within the FTC, CRSS data is used by attorneys, investigators, paralegals, data analysts, economists, and consumer protection counselors, for the purposes outlined in section 3.1, above. All internal users have read only access except for consumer counselors. Counselors also have the ability to enter consumer complaint information into the system and update consumer complaint records already entered, which they do when they receive updated information from the consumer complainant.

The FTC's contractor involved with the design, development, and maintenance of the system, Lockheed Martin Business Process Solutions, also has access to the CRSS data. In order to design and develop the CRSS system, LMBPS must analyze the data collected by the legacy FTC information systems. To maintain and support the ongoing CRSS operations including web portal hosting services and call center services, LMBPS staff must have access to the CRSS data. For example, a call center Customer Service Representative interacts directly with consumers and records the data into the CRSS system. Information confidentiality and Privacy Act requirements are specified in the service contract. In addition, CRSS must undergo certification and accreditation to ensure the security controls are properly implemented.

The FTC requires all of our contractors involved with data collection and processing, as well technical support of CIS, to undergo a rigorous security screening and clearance process, as well as sign a non-disclosure agreement.

LMBPS personnel accessing the CRSS system(s) receive initial training in security awareness

and accept security practices as part of their orientation. They also sign Rules of Behavior for the use of systems and applications prior to their being given access to those systems and applications. LMBPS personnel receive refresher training annually. Customer Service Representatives also receive security awareness training on sensitive information and PII information handling during orientation.

The LMBPS personnel with access to CRSS are aware of and understand the ramifications and penalties for infractions of the rules regarding privacy and data security. Any failure to comply with the Rules of Behavior is considered a security incident.

### **3.3 Which external entities will have access to the information?**

As part of its consumer protection mission, the FTC shares CRSS data with other law enforcement agencies (for a complete list, see <http://www.consumer.gov/sentinel/members.htm>). Through the CSN, CRSS data is shared with authorized local, state, federal, and international law enforcement agencies that have entered into a confidentiality and data security agreement with the FTC. This agreement requires, amongst other things, that CSN data will be accessed solely for law enforcement purposes. In addition, in response to specific law enforcement agency requests, the FTC will provide those agencies with data in an encrypted and password protected format, consistent with OMB and NIST standards.

As discussed previously, CRSS also limits users' access to the features, functions and data for which they are authorized. For example, the ability to extract data from CRSS will be limited to local, state and federal law enforcement agencies in the United States, Canada, and Australia, and will not be available to other foreign law enforcement users. Both the Office of International Affairs and the Office of General Counsel were consulted on the decisions involving sharing data with foreign entities.

Certain States that have entered into a Memorandum of Understanding with the FTC may download registered consumer telephone numbers from DNC for their State and use this information to update their State-specific do not call lists.

Telemarketers with currently valid subscriptions must, in accordance with the Telemarketing Sales Rule, access and download consumer telephone numbers in their subscription at least every 31 days to ensure that they do not call those numbers.

Pursuant to the Fair and Accurate Credit Transactions Act of 2003, Pub L. 108-159, 117 Stat. 1952, and the Commission's delegation of authority located at 68 FR 46642, the FTC shares certain consumer complaints (e.g. about the accuracy of a consumer's credit report) with

consumer reporting agencies (CRAs). The CRAs review the complaints, take appropriate actions, and report back to the Commission on their determinations. In addition, the CRAs will share selected complaints with consumer reporting agencies that maintain consumer files within the CRA system (“associated consumer reporting agencies” or “associated CRAs”). The CRAs will share with each associated CRA only those complaints that pertain to consumer files owned by that associated CRA, and will only share complaints with an associated CRA that has entered into a confidentiality agreement with the FTC. This information is shared in an electronic format, and is encrypted and password protected.

The FTC may be required or authorized to share complaint data with external entities in other circumstances, including in response to requests from Congress, Freedom of Information Act (FOIA) requests from private individuals or companies, requests from the media (not obtained through a FOIA request), or during litigation. Normally, in these situations, the FTC redacts all personally identifying information before providing the CRSS data. Government agencies also may request CRSS data for a non-law enforcement purpose (e.g., regulatory entities for licensing purposes). Such requests must be submitted to and approved by the Office of the General Counsel. Complaint data also may be shared with the entity about which a consumer complains in order to address the complaint. In the latter two situations, the FTC only discloses the data after receiving assurances of confidentiality from the recipients.

CRSS employs a number of technical and procedural safeguards, to protect the information that is shared with external entities. See section 2.6 for a discussion of some of the technical safeguards. In addition, as mentioned above, all CSN members are required to execute a confidentiality and data security agreement that outlines many of the CRSS procedural safeguards, as follows:

- CSN data will be accessed solely for law enforcement purposes;
- any information printed, downloaded or otherwise removed from the CSN (either in an electronic or in a printed format) must be properly protected (i.e. via NIST approved encryption tools for electronic data, or via a locked cabinet for paper based documents);
- any data extract must be destroyed within 90-days unless its use is still required for a valid law enforcement purpose;
- CSN information must be properly destroyed;
  
- CSN users may only access the system from computers issued and maintained by their organizations;
- CSN users may only access CSN from their official work stations;

- CSN users may only access the system from computers with up-to-date software, including anti-virus and anti-malware programs, a firewall, and properly patched operating system and application software;
- userids and passwords must be properly protected;
- CSN access and CSN information must only be provided to individual's with a need for such access and information;
- CSN members must notify the FTC in case of a data breach;
- CSN members must ensure that their staff understand their responsibilities under the agreement; and
- CSN users must complete a mandatory online training module prior to accessing the system.

#### **4.0 Notice and Access for Individuals**

##### **4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?**

Through notices available on the online complaint forms and through messages and menu items for the toll-free numbers, the FTC informs consumers that the information collected is not mandatory, but that if they do not provide certain information, it may be impossible for the FTC to refer, respond to, or investigate the consumer's complaint or request. The FTC Privacy Policy also informs consumers that any information they submit in connection with a complaint is voluntary.

The CIS is currently covered by two existing Privacy Act System of Records Notices (SORNs), FTC IV-1 (consumer complaints generally), and FTC IV-2 (ID theft portion), which will be merged. The FTC's SORNs, which are published in the Federal Register, are posted and accessible online through the FTC's Privacy Act page, <http://www.ftc.gov/foia/listofpaysystems.shtm>. In compliance with the Privacy Act, the Internet sites from which consumers can access the general and IDT complaint forms contain the required notice of authority, purpose, routine uses, and whether the collection is voluntary or mandatory. They also contain links to the FTC's Privacy Policy.

A program-specific Privacy Policy describes how the FTC handles the information collected from telemarketers, sellers and other entities when they visit DNC. The Privacy Act SORN corresponding to DNC records is currently designated FTC-IV-3 (National Do Not Call Registry® System-FTC), is published in the Federal Register, and is posted and accessible online through the FTC's Privacy Act page <http://www.ftc.gov/foia/listofpaysystems.shtm>. In compliance with the Privacy Act, the Internet sites and toll-free numbers from which consumers

can access DNC contain the required notice of authority, purpose, routine uses, and whether the collection is voluntary or mandatory. Both the consumer and telemarketer Internet sites also contain links to the FTC's privacy policy.

#### **4.2 Do individuals have the opportunity and/or right to decline to provide information?**

All information provided by consumers to the FTC is voluntary. Consumers may choose to submit some, all, or none of the information requested by the FTC's complaint forms. Consumers are informed that if they do not provide certain information, it may be impossible for the FTC to refer, respond to, or investigate the consumer's complaint or request.

Telemarketers must set up a profile by registering an account on the DNC system before they can access telephone numbers in the National Registry. To set up a profile, telemarketers must provide organizational information. If telemarketers decline to provide organizational information, they will not be able to set up a profile or gain access to telephone number information in the National Registry.

Law enforcement users requesting access to the CSN must go through a comprehensive and secure registration process and become approved and authorized members before being given access to the information available in the system. Law enforcement organizations and their users must provide the required information (see 2.1, above). If law enforcement users decline to provide the required information, they will not be able to complete the registration process, and they will not be given access to the CSN.

#### **4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?**

Consumers, telemarketers, and CSN law enforcement users do not have the right to consent to particular uses of their information. They consent to their information being provided for all uses described in the applicable privacy policies.

#### **4.4 What are the procedures that allow individuals to gain access to their own information?**

Consumers may request a copy of information covered by the Privacy Act, by following the FTC's Privacy Act rules and procedures, which are published in the Code of Federal Regulations at 16 C.F.R. 4.13. Consumers may update the information they provide in a complaint by following these procedures, or by calling the CRC at 1-877-FTC-HELP or 1-877-ID-THEFT. Consumers also may access their registration information by visiting the DNC website or by calling the DNC's toll-free telephone numbers. In addition, consumers may request to remove their telephone numbers from the DNC by calling the toll-free telephone numbers from the

telephone whose number they wish to remove. Telemarketers may correct their information by visiting the DNC website or by contacting the DNC Help Desk.

**4.5 If no formal procedure for individuals to access and/or correct their own information is provided, what alternatives are available to the individual?**

Not applicable.

**4.6 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.**

Requests by individuals for access to CRSS information are reviewed and evaluated by the FTC's FOIA office, in accordance with the FTC's Privacy Act rules and procedures, which are published in the Code of Federal Regulations at 16 C.F.R. 4.13 (see 4.4, above). In this regard, privacy risks inherent in the process are managed by the FTC's FOIA Office.

Requests made to the CRC by consumers wishing to update information they submitted are processed by CRC staff. To mitigate the risk that a consumer's information might be updated or shared with an unauthorized third party, the CRC requires callers to provide the unique reference number associated with the consumer's complaint, as well as other identifying details. Each complaint in CSN is assigned a unique reference number, which is provided to the consumer when a complaint is filed.

In addition, Consumers may access information related to their DNC registration by visiting the DNC website, or by calling the toll-free DNC telephone number. To mitigate the risk that a consumer's information might be altered or shared with an unauthorized third party, the DNC website employs a multi-step process, which includes the delivery of a confirmatory email. The website may only be used to register a telephone number, verify a registration, or file a complaint. Consumers cannot remove or delete a registration via the website. Consumers who use the toll-free DNC telephone number must call from the telephone number that is registered to access or change any DNC information.

**5.0 Web Site Privacy Issues**

**5.1 Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon).**

For system auditing purpose, CRSS collects and stores the following computer system and network related information:

- Date and time when the user gained access to CRSS
- Name of the domain and host from which the user gained access to CRSS
- Internet address of the site from which the user linked directly to the CRSS websites
- Internet protocol (IP) address of the computer the user was using
- User's web browser software information
- User's computer Operating System information

The computer system and network related information is used to determine the number of visitors to different sections of the CRSS websites, to help make the web sites more useful, to help ensure the proper operation of the web sites, and to help resolve helpdesk requests. This information is not used to track or record information about individuals.

CRSS web sites do not use persistent "cookies" or tracking mechanisms that collect personally identifying information. CRSS web sites do use session cookies on this site to anonymously collect a visitor's IP address and the date and time of the visit. Session cookies are temporary files that are erased when you close all browsers. We use these session cookies so that telemarketers, sellers, law enforcement agencies and other entities accessing the site can move from one secure Web page to another without having to log in to each page. Session cookies are mandatory to ensure the proper functioning of our site. Users may not be able to use the CRSS web sites if they decline to accept session cookies.

**5.2 If a persistent tracking technology is used, ensure certain issues are addressed.**

CRSS does not use persistent cookies or other persistent tracking devices on the system Web sites.

**5.3 If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.**

CRSS uses 128-bit SSL encryption when personal information is collected through a web site, page, or online form. Encryption also is applied to personal information, collected from consumers, telemarketers and law enforcement agencies, which is stored in the CRSS database.

**5.4 Explain how the public will be notified of the Privacy Policy.**

Privacy policy information is made available to the public via a hyperlink on every CRSS web site. The CRSS privacy policy is machine-readable (i.e. P3P compliant), and handicap accessible pursuant to Section 508 of the Rehabilitation Act.

**5.5 Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.**

The FTC has identified privacy risks associated with CRSS and has taken steps to mitigate those risks. With respect to the collection of data, the identified risks are:

- Consumers might not understand how their information will be used
- CRSS might collect more information than is required (e.g., consumers provide SSNs on the general complaint form when not needed)

**NOTE: Privacy risks and mitigation are discussed in various sections throughout this document, including sections 2.8, 3.1, 3.2, 3.3, 4.1, 4.6, 5.5, and 7.3.**

To address these risks, CRSS provides notices (on the online complaint forms and through telephone counselors) about how consumers' information will be used. On the online complaint forms, CRSS provides a link to the FTC's privacy policy. Social Security Numbers, if provided, are encrypted when stored in CRSS. CRSS also explains on the general complaint form that a Social Security Number should be provided only for certain types of complaints.

**5.6 If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).**

CRSS Web sites are not directed to children under the age of 13, and if an individual lodges a complaint and indicates that he/she is under the age of 13, CRSS deletes and purges any personally identifying information in that complaint. However, CRSS web sites accept identity theft complaints filed on behalf of a minor by an adult.

**6.0 Security of Information in CRSS**

**6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?**

CRSS employs both information security and physical security to protect the privacy related information it collects. CRSS complies with OMB and NIST standards, as well as FTC security policies.

**6.2 Has a Certification & Accreditation been completed for the system or systems supporting the program?**

To ensure CRSS meets US government information security standards, the FTC mandates the following information security practices:

- Adherence to IT security requirements and procedures as required by federal law and policy to ensure that information is appropriately secured;
- Completion of a risk assessment that identifies appropriate security controls, and implementation of the controls;
- Completion of all security related activities required by the Commission's Certification and Accreditation Policy, including:
  - Completion of a risk assessment to identify appropriate security controls and development of a system security plan to document the managerial, technical and operational controls used by the system;
  - Completion of security testing and evaluation of the system by an independent party to verify that the specified controls are in place and operating as expected;
  - Monthly scanning of the system to ensure that implemented controls continue to operate as expected and to identify and mitigate any new vulnerability;
  - A 'self-assessment' evaluation of risk to the system on an annual basis and development of a new risk assessment and system security plan every three years or when there are significant changes to the architecture of the system;
  - Designation of the Office of Information Technology, Office of the Executive Director, Federal Trade Commission, as the point of contact for questions about the technical controls on this system.

### **6.3 Has a risk assessment been conducted on CRSS?**

As part of the CRSS Certification and Accreditation process, a Risk Assessment has been conducted on CRSS. Appropriate security controls have been identified and implemented to protect against the identified risk. Any residual risk will be documented in the CRSS Plan of Action and Milestone document.

### **6.4 Does CRSS employ technology that may raise privacy concerns? If so, please discuss its implementation.**

No. The technology employed by CRSS does not raise any special privacy concerns not already addressed.

**6.5 What procedures are in place to determine which users may access the system and are they documented?**

All CRSS users, including FTC staff, external law enforcement members, call center staff, data providers, and data receivers, access their relevant and authorized features and functions through a secured and personalized portal interface on the CSN. Because of different needs, these varied group of CRSS users access information under different security policies.

FTC staff and external law enforcement members access CRSS information through respective portal interfaces. In accordance with OMB and NIST standards, access to the CRSS CSN portal will be strictly controlled, and will utilize a minimum of two authentication factors. Authentication factors will include, unique user names, passwords, one-time passcodes generated by RSA SecureID tokens, approved IP address ranges, and such other factors as the FTC may determine are necessary to ensure the confidentiality and security of the system and its data.

Data contributors and data receivers are also authenticated if they access CRSS to either contribute or receive data. Their access is restricted to only uploading or downloading of data.

**6.6 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.**

The LMBPS personnel managing or accessing the CRSS systems have received initial training in security awareness and accepted security practices as part of their orientation and sign Rules of Behavior for the use of systems and applications prior to their being given access to those systems and applications. LMBPS personnel receive refresher training annually.

Consumer Service Representatives from the CRC also receive security awareness training on sensitive information and PII information handling during orientation.

For CRSS CSN users, a mandatory online training course on PII data handling must be taken prior to first use and repeated annually. Training record information is kept online as part of the user profile.

**6.7 What auditing measures and technical safeguards are in place to prevent the misuse of data?**

CRSS limits users' access to data and functions based on their role. Each user is assigned a unique user name and password (passwords must be strong - i.e., at least 8 characters; contain a mix of letters, numbers and special characters; and not be based on a word in any language, slang or jargon). Access to CRSS is password protected. Access to the CSN requires dual verification - a SecureID token number and a password. In addition, by using granular access

and authorization techniques, users are limited only to the features and functions they can use and have access only to specific subsets of the data. For example, the contractors involved with data collection can only view the data which they enter, and CPS users only can view data received through econsumer.gov. Users cannot see Social Security Numbers. External law enforcement members access CRSS through 128-bit SSL encryption and strong two factor authentication. The FTC also maintains audit logs of each user's activity in CRSS.

All sensitive data is encrypted during transmission from the CRSS portals to the end users or external systems using 128-bit Secure Sockets Layer (SSL) encryption via Secure Hyper Text Transfer Protocol (HTTPS). All data at rest is encrypted using state-of-the-art hardware encryption technology. All user access and operations are logged. Microsoft enterprise library and other system logs are used to register the user operation and stored in a central repository. The logs are used to audit the user access and produce security reports periodically. The CRSS application network perimeter is protected through advanced firewalls and the Intrusion Detection System (IDS).

The CRSS application is monitored 24x7 for any type of security intrusion attempts. All security issues are reported either immediately or routinely, depending on the severity of the issue, to authorized FTC personnel for analysis and appropriate actions.

The CRSS system is hosted at a primary data center, a reliable, secure, and well-managed hosting facility from Lockheed Martin BPS located in Rockville, Maryland. A secondary data center for disaster recovery and business continuity will be housed in an advanced data center facility located in Denver, CO, providing for adequate geographical separation from the primary data center. Call center functionalities are provided by the primary call center in Indianapolis, IN and the backup call center in Albuquerque, NM.

## **7.0 DATA RETENTION**

### **7.1 For what period of time will CRSS data be maintained?**

At this time, all CRSS information - including consumer complaints, telemarketer information, and system data - is maintained indefinitely, except for the following:

- Letters and correspondence from consumers received via the mail are retained for one year, and then destroyed.
- Any media received from a CRSS data contributor is destroyed in accordance with OMB and NIST guidelines 90-days after the data is imported into CRSS.

The FTC is preparing and plans to submit to the National Archives and Records Administration (NARA) a comprehensive records disposition schedule which will replace the FTC's current records schedules and will schedule previously unscheduled items including electronic systems

such as CRSS. As part of the process of preparing the comprehensive records schedule, the agency is determining retention periods for data in CRSS. Pending submission of the comprehensive records schedule to NARA and NARA's approval of the schedule, FTC continues to manage CRSS in a manner consistent with 44 U.S.C. ch. 31, 44 U.S.C. 3506, 36 CFR Ch. XII, Subchapter B, Records Management, and OMB Circular A-130, par. 8a1(j) and (k) and 8a4.

## **7.2 What are the plans for destruction or disposal of the information?**

All CRSS information that is subject to disposal (see 7.1, above) will be destroyed in accordance with OMB and NIST guidelines.

## **7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.**

To mitigate the risks of unauthorized access or sabotage of privacy data stored in CRSS, data encryption technology is employed to secure data stored on CRSS systems. Media received from CRSS data contributors is stored for 90 days after information on the media has been imported into CRSS and is then destroyed in accordance with OMB and NIST guidelines.

## **8.0 Privacy Act**

### **8.1 Will the data in the system be retrieved by a personal identifier?**

Yes. Consumer complaint data can be retrieved by the following fields:

- Consumer Name
- Street Address
- EIN or SSN
- Telephone Number
- Email Address
- Unique FTC Reference Number

Telemarketer information can be retrieved by the following fields:

- Organization Name
- Street Address
- EIN or SSN
- Telephone number
- First Name or Last Name
- Email Address

**NOTE: Telemarketer business entities are not covered by the Privacy Act.**

For two categories of consumer complaints, identity theft-related complaints and complaints related to the accuracy of the consumer's credit report, CIS allows the consumer to provide a Social Security Number. CIS encrypts the SSN, and the number is not displayed when users search the system. However, the system allows users to search for complaints by SSN.

**8.2 Is the system covered by an existing Privacy Act System of Records notice (SORN)?**

The CIS is currently covered by two existing Privacy Act System of Records Notices (SORNs), FTC IV-1 (consumer complaints generally), and FTC IV-2 (ID theft portion), which will be merged. The FTC's SORNs, which are published in the Federal Register, are posted and accessible online through the FTC's Privacy Act page, <http://www.ftc.gov/foia/listofpaysystems.shtm>. In compliance with the Privacy Act, the Internet sites from which consumers can access the general and IDT complaint forms contain the required notice of authority, purpose, routine uses, and whether the collection is voluntary or mandatory. They also contain links to the FTC's Privacy Policy.

The DNC is currently covered by one Privacy Act SORN, which is currently designated FTC-IV-3 (National Do Not Call Registry<sup>®</sup> System-FTC), is published in the Federal Register, and is posted and accessible online through the FTC's Privacy Act page <http://www.ftc.gov/foia/listofpaysystems.shtm>. In compliance with the Privacy Act, the Internet sites and toll-free numbers from which consumers can access DNC contain the required notice of authority, purpose, routine uses, and whether the collection is voluntary or mandatory. Both the consumer and telemarketer Internet sites also contain links to the FTC's privacy policy.

**9.0 Privacy Policy**

The collection, use, and disclosure of CRSS information has been reviewed to ensure consistency with the FTC's privacy policy.

**10.0 Approval and Signatures**

This Privacy Impact Assessment document must be signed and approved by Federal Trade Commission and Lockheed Martin. Please sign and date to acknowledge review of this document.

**Federal Trade Commission**

---

David Torok  
Associate Director  
Division of Planning and Information  
Bureau of Consumer Protection

---

Margaret Mech  
Chief Information Security Officer

---

Kathy French  
Assistant Director - COTR

---

Alexander C. Tang  
Attorney, Office of General Counsel

---

Marc Groman  
Chief Privacy Officer

---

Stanley Lowe  
Chief Information Officer

**Lockheed Martin**

---

Thomas Martwinski  
Program Manager

---

Keith Myers  
Chief Information Security Officer  
Chief Privacy Officer