

Part I: i-SAFE and the i-SAFE Harbor Program

I (A) i-SAFE Inc.

Background: In order to protect children and teens from the personal and social dangers associated with their use of the Internet, the Congress joined with i-SAFE to bring e-Safety education to K-12 students nationwide (and students in Department of Defense schools worldwide). This has been a massive and comprehensive effort to equip the children and teens of families throughout the nation (and those temporarily overseas) with the critical thinking and decision-making skills they need in order to be able to recognize and avoid dangerous, destructive and unlawful online behavior and to conduct themselves appropriately and safely.

Congress first funded i-SAFE in 2002 and, since that time, i-SAFE has provided world-class e-Safety education and programming to more than 6.5 million students in more than 13,700 schools, including more than 100,000 military dependent students in 221 Department of Defense (DoDEA) schools in 13 foreign countries. In 2009, i-SAFE is projected to provide e-Safety education and programming to 10 million U.S. students!

i-SAFE is a highly efficient non-profit organization that successfully partners with industry leaders (e.g., Microsoft, Verizon, Yahoo, VeriSign, etc.), schools, law enforcement agencies, parents organizations and others to enable citizens in all 50 states to remain safe from online predators, consumer fraud, bullying, and many other online victimization schemes. i-SAFE has a very broad reach and works cooperatively with many different types of organizations to promote e-Safety. Several notable examples include:

- In 2008, many government and non-government organizations were awarded competitive federal grants to use and disseminate i-SAFE's e-Safety intellectual property to students, educators, law enforcement professionals and parents and senior citizens.
- i-SAFE is partnered with the American Football Coaches Association (AFCA) to deliver the AFCA's Child ID Kits to students throughout the United States, and partnered with the United States Patent and Trademark Office (USPTO), the Federal Trade Commission (FTC), Recording Industry Association of America (RIAA), and American Society of Composers, Authors and Publishers (ASCAP) to provide e-Safety education that helps prevent devastating financial losses to the billion dollar music and movie industries by educating consumers (young and mature) on the illegalities of copyright infringement and piracy.
- i-SAFE operates the National Assessment Center (NAC) database, which is the world's largest repository of real-time (and historical) data on K-12 student online attitudes and behaviors. The NAC's data (metrics) are shared with the FBI, local law enforcement, education institutions, and industry leaders and provides the linkage resources for connecting law enforcement with individual users of technology in the larger context of the ever-changing technologies and behaviors in the digital world.

On October 21, 1998, Congress enacted COPPA (Children’s Online Privacy Protection Act) to prohibit unfair or deceptive acts or practices in connection with the collection, use or disclosure of personally identifiable information from and about children on the Internet. Section 6502 of the Act requires the FTC to enact rules governing the online collection of personal information from children under age 13 within one year of the date of the enactment of the COPPA. The FTC published a Notice of Proposed Rulemaking and Request for Public Comment in the FEDERAL REGISTER on April 27, 1999, and the 45-day comment period closed on June 11, 1999. Following public comment and a public workshop, the FTC issued its Final Rule (the “Rule”) which became effective on April 21, 2000.

Section 312.10 of the Rule provides that an operator’s compliance with FTC-approved self-regulatory guidelines serves as a safe harbor in any enforcement action for violations of the Rule. To receive safe harbor treatment, an operator can comply with any FTC-approved guidelines. The operator need not independently apply for approval if in fact the operator is fully complying with guidelines already approved by the Commission that are applicable to the operator’s business.

As of September 2008, four “safe harbors” have been FTC-approved: 1) The Children’s Advertising Unit (CARU) of the Council of Better Business Bureaus, Inc.; 2) ESRB Privacy Online, A Division of Entertainment Software Rating Board (ESRB); 3) TRUSTe; and 4) Privo, Inc. In 2008, as an extension of its e-Safety programs, i-SAFE determined it, too, would become available to assist operators deal sensitively with, and protect the privacy of, children online by meeting and/or exceeding the requirements of the Rule through compliance with FTC-approved i-SAFE Harbor Guideline Requirements.

I (B) i-SAFE Harbor program

Introduction: i-SAFE Harbor is a safe harbor information privacy seal program that provides parents and children with the assurance they have the ability to manage their personal information that Web sites obtain from them. The foundation of this assurance is the fact that i-SAFE Harbor is an information privacy compliance and enforcement program that assists commercial enterprises in protecting the personal information they obtain online from children and invests them with the confidence that the information they obtain from children online is compliant with COPPA (i.e., collected, used and disclosed in a secure, reliable manner consistent with current statutory law). The following sections describe the major programmatic elements of the i-SAFE Harbor program:

Guideline Requirements: i-SAFE Harbor Participant/Licensees must agree to abide by i-SAFE Harbor Guideline Requirements. i-SAFE Harbor Guideline Requirements are a set of guidelines that regulate how i-SAFE Harbor Participant/Licensees collect, use and disclose personal information from children 12 years old and younger. By following i-SAFE Harbor Guideline Requirements, visitors to Web sites operated by i-SAFE Harbor Participant/Licensees are assured that:

- A *Privacy Policy* will be posted on the homepage of an i-SAFE Harbor Participant/Licensee's Web site and provide a link to such *Privacy Policy* at each point within the Web site where personal information is collected;
- Notice will be provided to the child's parent about the Web site's information practices and prior verifiable consent will be obtained before collecting personal information from children;
- The child's parent will be given the choice to consent to the collection and use of their child's personal information for internal use by the Web site; and, the parent will be given the opportunity to elect not to have their child's personal information disclosed to third parties;
- The parent will be provided with access to their child's personal information and given the ability to delete the information and opt-out of the future collection or use of the information;
- The child's participation in an activity will not be conditioned on the child's disclosure of more personal information than is reasonably necessary for the activity; and
- i-SAFE Harbor Participant/Licensees will maintain the confidentiality, security and integrity of the personal information they collect from children.

Compliance Assessment Checklist (CAC): Prospective i-SAFE Harbor Participant/Licensees (i.e., applicants) must complete an initial i-SAFE Harbor ***CAC***. Completion and submission of the ***CAC*** constitutes a self-evaluation (i.e., assessment) of the prospective Participant/Licensee's Web site and information *Privacy Policies* and business practices (i.e., personal information collection, use and disclosure). The ***CAC*** also helps prospective i-SAFE Harbor Participant/Licensees prepare for the i-SAFE Harbor Qualification Audit Review. i-SAFE Harbor Participant/Licensees also must complete and submit to i-SAFE an updated ***CAC*** annually.

Qualification Audit Review (QAR): As part of i-SAFE Harbor Guideline Requirements, i-SAFE Harbor Participant/Licensees must post a *Privacy Policy* that is clear, understandable and contains no unrelated contradictory or confusing material. To assist i-SAFE Harbor Participant/Licensees in implementing a meaningful and trustworthy *Privacy Policy* that properly conveys to parents and children the necessary information about the Web site's operator's information practices, i-SAFE offers i-SAFE Harbor Participant/Licensees guidance on how to modify their existing *Privacy Policy* or, in the alternative, helps them draft their first *Privacy Policy* to ensure they comply with i-SAFE Harbor Guideline Requirements. To become an i-SAFE Harbor Participant/Licensee, Web site operators must successfully pass a ***QAR***, which is conducted by i-SAFE and involves a thorough examination of an applicant's ***CAC***, Web site and current information practices. During the ***QAR***, i-SAFE:

1. Determines whether or not the prospective Participant/Licensee's privacy statement is an accurate representation of its internal and external information practices;
2. Ensures the prospective Participant/Licensee's information practices meet all i-SAFE Harbor Guideline Requirements; and
3. Assesses the likelihood that the prospective licensee will continue to meet the i-SAFE Harbor Guideline Requirements on a consistent basis.

Participant License Agreement (PLA): i-SAFE Harbor applicants that successfully pass the ***QAR***, must execute an i-SAFE Harbor ***PLA***, which obligates them to fully meet and comply with all i-SAFE Harbor Guideline Requirements (See i-SAFE Harbor Program Guideline Requirements #1-7), including the i-SAFE Harbor Compliance Enforcement Program and Complaint/Dispute Resolution Process. A Participant/Licensee's failure to comply with i-SAFE Harbor Guideline Requirements may constitute a material breach of the ***PLA*** and also a trademark infringement and a dilution of the goodwill and reputation associated with the i-SAFE Harbor logogram ("emblem"). i-SAFE Harbor Participant/Licensees are authorized to use the i-SAFE Harbor emblem only in accordance with the terms and conditions of the ***PLA***.

i-SAFE Harbor Emblem: i-SAFE Harbor Participant/Licensees that meet and comply with i-SAFE Harbor Guideline Requirements are licensed to display the i-SAFE Harbor emblem (i.e., a safe harbor privacy seal). For parents and children, the i-SAFE Harbor emblem offers them assurance that the Web site has a posted *Privacy Policy*, that the *Privacy Policy* accurately and completely describes how personal information is collected, used and disclosed and that Web site submits to ongoing monitoring and enforcement of their Web site's compliance with FTC approved i-SAFE Harbor Guideline Requirements. Visitors to Web sites whose operators are i-SAFE Harbor Participant/Licensees can verify such membership (in good standing) by using the "click-on" feature of the i-SAFE Harbor emblem. Each i-SAFE Harbor emblem is linked to a verification page on a secure i-SAFE server. The verification page allows parents to verify that the Web site is authorized to display the i-SAFE Harbor emblem and currently is in good standing and full compliance with i-SAFE Harbor Guideline Requirements.

Periodic Monitoring: Periodic monitoring is a key assessment mechanism feature of the i-SAFE Harbor program and includes the following components: 1) initial and annual self-assessments of i-SAFE Harbor Participants'/Licensees' Web sites (e.g., the ***CAC***); 2) an initial ***QAR*** (Qualification Audit Review) followed by periodic unannounced monitoring reviews (i.e., independent assessments) of i-SAFE Harbor Participants'/Licensees' Web sites; and 3) community assessment (i.e., queries, complaints and complaint resolution).

First, all i-SAFE Harbor Participant/Licensees must conduct an initial self-assessment of their Web site's information collection, use and disclosure practices. Each i-SAFE Harbor Participant/Licensee is required to complete and attest to the accuracy of the statements they make on a self-assessment form about their information practices (i.e., the ***CAC***). A representative of the i-SAFE Harbor program will independently review the Web site's *Privacy Policy* and practices with the applicant's self-assessment form (i.e., the ***QAR***) to ensure they are consistent with: 1) each other; 2) the i-SAFE Harbor Guideline Requirements; and 3) COPPA.

Before becoming a Participant/Licensee in the i-SAFE Harbor program, the company/Web site operator seeking to become an i-SAFE Harbor Participant/Licensee must make all required modifications to their Web site that i-SAFE deems necessary to comply with i-SAFE Harbor Guideline Requirements and COPPA. i-SAFE Harbor Participant/Licensees will be required to complete the self-assessment form (CAC) on an annual basis to ensure their Web site information practices continually comply with i-SAFE Harbor Guideline Requirements and COPPA and are consistent with their Web site's posted *Privacy Policy*.

Second, all i-SAFE Harbor Participant/Licensees must submit to quarterly or semi-annual or annual monitoring reviews of their Web site's information practices. The purpose of monitoring reviews is to ensure that an i-SAFE Harbor Participant/Licensee's Web site and its *Privacy Policy* are constantly in full compliance with i-SAFE Harbor Guideline Requirements and COPPA. Specifically, monitoring reviews are conducted by trained privacy monitors that systematically move about an i-SAFE Harbor Participant/Licensee's Web site to ensure: 1) there is prominent link to the Web site *Privacy Policy* on the homepage and any Web page where information is collected by the Web site; 2) the i-SAFE Harbor Participant/Licensee obtains prior verifiable parental consent from children 12 years old and younger before collecting their personal information; and 3) general compliance with i-SAFE Harbor Guideline Requirements.

In addition to quarterly or semi-annual or annual monitoring, i-SAFE Harbor Participant/Licensees also must agree to submit to periodic, unannounced monitoring reviews of their Web site(s). These unannounced reviews are conducted to further verify that the i-SAFE Harbor Participant/Licensee's Web site is complying with i-SAFE Harbor Guideline Requirements and COPPA at all times. i-SAFE Harbor "information privacy monitors" also will periodically "seed" Participant/Licensee's Web sites with personal information to actually test the manner in which the Web site collects, uses and discloses it and to ensure the i-SAFE Harbor Participant/Licensee is not using personal information for any other purposes than stated in its *Privacy Policy*. Each quarterly or semi-annual or annual or periodic review is memorialized in a written report and maintained by i-SAFE for a period of three (3) years.

Third, all i-SAFE Harbor Participant/Licensees must provide parents and children with a reasonable and effective means to submit complaints about an i-SAFE Harbor Participant/Licensee's information practices. The i-SAFE Harbor third-party complaint/dispute resolution program also offers parents and children the opportunity and mechanism to submit complaints about any i-SAFE Harbor Participant/Licensee's Web site directly to i-SAFE Harbor representatives. i-SAFE maintains a record for three (3) years of all complaints/disputes, including any investigation conducted by i-SAFE into alleged violations of i-SAFE Harbor Guideline Requirements, any third-party complaint/dispute resolutions conducted by i-SAFE and the outcome of such investigation(s) and third-party resolutions.

Complaint/Dispute Resolution Process: INTERNAL RESOLUTION – i-SAFE Harbor Participant/Licensees must create and implement a complaint/dispute resolution program, internal to their business operations, which should be designed to fairly and expeditiously resolve privacy related issues and complaints raised by consumers or by i-SAFE (i.e., a means for parents and children to submit queries or complaints they may have about an i-SAFE Harbor Participant/Licensee's information practices). THIRD-PARTY RESOLUTION – If consumers

are not satisfied with the response they receive from an i-SAFE Harbor Participant/Licensee, i-SAFE Harbor offers them third-party assistance in resolving their complaints/disputes. i-SAFE Harbor Participant/Licensees are contractually compelled (i.e., in the *PLA*) to resolve privacy complaints/disputes and violations using the i-SAFE Harbor third-party complaint/dispute resolution process when consumer grievances are not effectively addressed through the Participant/Licensee's own internal complaint/dispute resolution mechanism/program. i-SAFE Harbor Participant/Licensees are required to fully participate in any inquiry or investigation conducted by i-SAFE Harbor representatives, and they are bound to abide by i-SAFE Harbor third-party complaint/dispute resolution final determinations, rulings, and/or decisions.

I (C) Summary/Restatement of i-SAFE Harbor Guideline Requirements (See full text at TAB 2)

As a worldwide e-Safety education and programming provider, i-SAFE fully appreciates the importance of maintaining a safe and secure environment for children online. To help facilitate this type environment for children online, the following seven (7) i-SAFE Harbor Guideline Requirements must be followed by i-SAFE Harbor Participant/Licensees when operating Web sites directed in whole or in part to children who are 12 years old and younger and when collecting information from children or have actual knowledge they collect information from children 12 years old and younger:

Requirement #1: Notice/Disclosure of Information

i-SAFE Harbor Participant/Licensees that collect personal information from children 12 years old or younger must post a prominent link that is clearly labeled *Privacy Policy* or such similar notice that links the children to a description of the Participant/Licensee information collection, use and disclosure practices.

The *Privacy Policy* link must be placed in a clear and prominent place and manner on the homepage of the Participant/Licensee's Web site (or online service) and at each area where personal information is collected from children – and in close proximity to the requests for personal information in each such area.

Privacy Policies must be clear and understandable and should not contain unrelated, contradictory or confusing material. *Privacy Policies* must describe the following information:

Participant/Licensee Contact Information: i-SAFE Harbor Participant/Licensees must include their complete contact information. Such information must include the name, mailing address, telephone number and e-mail address. In cases where more than one company is responsible for a Web site, the Participant/Licensee may choose to respond to all inquiries from parents concerning the Participant/Licensee's *Privacy Policy*, provided that the names of all persons or companies collecting personal information through the Web site are listed.

Types of Personal Information Collected: i-SAFE Harbor Participant/Licensees must describe the types of personal information collected and whether the personal information is collected directly or passively.

Use of Personal Information: i-SAFE Harbor Participant/Licensees must describe how personal information is used.

Disclosure of Personal Information: i-SAFE Harbor Participant/Licensees must state whether personal information is disclosed to third parties. If the Participant/Licensee does disclose personal information, the Participant/Licensee must: 1) describe the types of business in which such third parties are engaged and the general purposes for which the information is used; 2) whether the third parties have agreed to maintain the confidentiality, security and integrity of the personal information they obtain from the Participant/Licensee; and 3) that parents have the option to consent to the collection and use of their children's personal information without consenting to the disclosure of that information to third parties.

Control Over Personal Information: i-SAFE Harbor Participant/Licensees must state in their *Privacy Policy* the choices available to parents and children regarding how children's personal information is collected and used.

Restrictions on Information Collection: i-SAFE Harbor Participant/Licensees must state they are prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

Access to Information: i-SAFE Harbor Participant/Licensees must state that parents can review their child's personal information, update their child's information, have such information deleted, and refuse to permit further collection or use of their child's information. Participant/Licensees also must describe the procedures parents must follow to access their child's personal information.

Queries/Complaints: i-SAFE Harbor Participant/Licensees must state in their *Privacy Policy* where parents or children can address any queries or complaints they have concerning the Participant/Licensee's Web site information practices.

Requirement #2: Direct Notice to Parents

i-SAFE Harbor Participant/Licensees must make reasonable efforts to ensure parents receive notice of the Participant/Licensee's information collection, use and disclosure practices with regard to their children, including notice of any material change in the collection, use or disclosure practices to which a parent had previously consented.

Direct notices to parents must contain the following information:

A. Privacy Policy Information: i-SAFE Harbor Participant/Licensees must include all of the information that is necessary to meet Requirement #1 above.

B. Purpose is to Collect Information: i-SAFE Harbor Participant/Licensees must affirmatively state they wish to collect personal information from the parent's child.

C. Parental Consent Required: i-SAFE Harbor Participant/Licensees must affirmatively state that the parent’s consent is required for the collection, use or disclosure of their child’s personal information. Participant/Licensees also must provide the method by which parents may give such consent.

Except for certain circumstances (i.e., exceptions) described in Requirement #3(C) below, i-SAFE Harbor Participant/Licensees must meet the requirements described above and obtain prior verifiable parental consent before they are allowed to collect personal information from children.

Requirement #3: Prior Verifiable Parental Consent

A. Generally, i-SAFE Harbor Participant/Licensees must obtain verifiable parental consent before any collection, use or disclosure of personal information from children. They also must obtain such consent when there is any material change in the collection, use or disclosure practices to which a parent has previously consented.

B. Methods for Obtaining Prior Verifiable Parental Consent: Any method to obtain prior verifiable parental consent must be reasonably calculated, in light of the available technology, to ensure that the person providing consent is the child’s parent.

1. **WHEN PERSONAL INFORMATION OF A CHILD AGE 12 AND YOUNGER IS MADE PUBLICLY AVAILABLE** the methods to obtain prior verifiable parental consent include: 1) providing a consent form to be signed by the parent and returned to the i-SAFE Harbor Participant/Licensee by postal mail or facsimile; 2) requiring the parent to use a credit card in connection with a transaction; 3) requiring the parent to send an e-mail containing the parent’s digital signature; 4) having a parent call a toll-free telephone number staffed by trained personnel; or 5) obtaining an e-mail with a PIN or password acquired through one of the four (4) verification methods above.

2. **WHEN PERSONAL INFORMATION OF A CHILD AGE 12 AND YOUNGER IS USED ONLY FOR INTERNAL PURPOSES** (i.e., the personal information will not be disclosed to third parties or made publicly available) the methods to obtain prior verifiable parental consent include the 5 methods listed in paragraph B.1. above and also by the “email plus” method.¹ The “email plus” method allows i-SAFE Harbor Participant/Licensees to request (in the direct notice to parents) that the parent provide consent in an email message AND, after receiving the parent’s email consent, then confirming that it was, in fact, the parent who provided consent by taking the following additional (the “plus”) steps:

- Requesting in the Participant/Licensee’s initial email seeking consent that the parent include a phone or fax number or mailing address in the reply email, so that Participant/Licensees can follow up to confirm consent via telephone, fax, or postal mail; or
- After a reasonable time delay, sending another email to the parent to confirm consent. In this confirmatory email, Participant/Licensees should include all the

¹ NOTE: i-SAFE will discourage i-SAFE Harbor Participant/Licensees from using the email plus method and strongly encourage them to use any of the five other more reliable methods of obtaining verifiable parental consent.

original information contained in the direct notice, inform the parent that he or she can revoke the consent, and inform the parent how to revoke the consent.

i-SAFE Harbor Participant/Licensees must give parents the option to consent to the collection and use of their child's personal information without consenting to disclosure of that information to third parties.

C. Exceptions to Prior Verifiable Parental Consent: Even though prior verifiable parental consent is required under most situations before an i-SAFE Harbor Participant/Licensee is permitted to collect, use or disclose a child's personal information, there are a limited number of exceptions where a Participant/Licensee will be allowed to collect a child's first name or online contact information before obtaining consent from the child's parent. The exceptions to prior verifiable parental consent are as follows:

- **Required Parental Consent** – i-SAFE Harbor Participant/Licensees may collect the name or online contact information of a parent to be used for the sole purpose of obtaining parental consent. If a Participant/Licensee has not obtained parental consent after a reasonable time (i.e., from the date of the information was collected), the Participant/Licensee must delete such information from its records. Participant/Licensees that collect the name or online contact information from a parent under this exception must provide direct notice to the parent. The direct notice must include all *Privacy Policy* information [See Requirement #2(A) above] and notify the parent the i-SAFE Harbor Participant/Licensee has collected their name and e-mail address to respond to and obtain consent from the parent. If the Participant/Licensee has not obtained parental consent after a reasonable time from the date the information is collected, the i-SAFE Harbor Participant/Licensee must delete such information from its records.
- **One-Time Request** – i-SAFE Harbor Participant/Licensees may collect the online contact information (e.g., email address) of a child for the sole purpose of responding directly, on a one-time basis, to a specific request from the child. Participant/Licensees that collect the online contact information from a child under this exception must not use the information to re-contact the child after the initial response and must delete the child's online contact information. *Direct notice is not required under this exception.*
- **Multiple Requests** – i-SAFE Harbor Participant/Licensees may collect the online contact information from a child to be used to respond directly more than once to a specific request from the child so long as the information is not used for any other purpose. Participant/Licensees that obtain the online contact information from a child under this exception must provide direct notice to the parent. The direct notice must: 1) include all *Privacy Policy* information [See Requirement 2(A) above]; 2) notify the parent that the Participant/Licensee has collected their child's online contact information in order to respond to their child's request; 3) explain the nature and intended use of the information; 4) inform the parent they may request the Participant/Licensee make no further use of the information and that such information be deleted; 5) describe the procedures by which the parent can refuse to allow further contact and information collection from their child; and 6) explain that if the parent does not opt-out, the i-SAFE

Harbor Participant/Licensee may use the information for the purposes stated in the direct notice. The direct notice to the parent must be sent after the initial response and before making any additional response to the ir child.

- ***Child Safety*** – i-SAFE Harbor Participant/Licensees may collect a child’s first name or online contact information to the extent reasonably necessary to protect the safety of a child participant on the Web site where the Participant/Licensee used reasonable efforts to provide notice to the parent. The information collected by the i-SAFE Harbor Participant/Licensee under this exception must be used for the sole purpose of protecting the child’s safety, must not be used to re-contact the child or for any other purpose than for the purpose stated in this exception and must not be disclosed by the i-SAFE Harbor Participant/Licensee on its Web site. The direct notice must: 1) include all *Privacy Policy* information [See Requirement #2(A) above]; 2) notify the parent that the Participant/Licensee has collected their child’s online contact information to protect the safety of the ir child participating on the Web site; 3) inform the parent they may refuse to permit the use of the information and may require its deletion, and inform them how they can have the information deleted; and, 4) explain that if the parent does not opt-out, the i-SAFE Harbor Participant/Licensee may use the information for the purposes stated in the direct notice.
- ***Additional Safety Concerns*** – i-SAFE Harbor Participant/Licensees may collect a child’s first name or online contact information to protect the security or integrity of its Web site, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or investigations on matters related to public safety so long as the information is not used for any other purpose. Direct notice is not required under this exception.

Requirement #4: Access and Review

i-SAFE Harbor Participant/Licensees must provide parents with the ability to access and review their child’s personal information. Parental review and access must consist of: 1) a description of the specific types of personal information collected from their child; 2) the opportunity at any time to refuse to permit the Participant/Licensee further using or collecting their child’s personal information; and 3) the ability to direct the Participant/Licensee to delete their child’s personal information from the Participant/Licensee’s records.

In addition to providing the ability for a parent to access and review their child’s personal information, i-SAFE Harbor Participant/Licensees must take reasonable steps to ensure the individual requesting access is the parent of the child. Acceptable steps for authenticating the identity of the parent online include a username and password unique to the parent or, if access is requested over the telephone, asking a series of questions about which only a parent of the child would have knowledge (e.g., parent’s name, mailing address or email address; or the child’s name, email address, etc.).

Requirement #5: Restrictions on Information Collection

i-SAFE Harbor Participant/Licensees are prohibited from conditioning a child's participation in an activity upon the child disclosing more personal information than is reasonably necessary to participate in such activity.

Requirement #6: Confidentiality, Security and Integrity of Information

i-SAFE Harbor Participant/Licensees must establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children.

Requirement #7: Compliance/Enforcement

A. Program Representatives: i-SAFE Harbor Participant/Licensees must appoint a program representative for their Web site(s). The program representative shall be the individual responsible for overseeing the Web site's compliance with i-SAFE Harbor Guideline Requirements. Program representatives shall be given the authority to investigate, in a timely manner, all inquiries concerning the Web site's *Privacy Policy* and information practices.

B. Initial and Annual Self-Evaluation: i-SAFE Harbor Participant/Licensees must conduct a self-evaluation (i.e., assessment) of their Web site information collection, use and disclosure practices (i.e., the *CAC*). Each Participant/Licensee is required to complete and attest to the accuracy of the statements made in the *CAC* self-evaluation form concerning their information practices. When i-SAFE receives a *CAC*, an i-SAFE Harbor representative will independently review the respective Web site's posted *Privacy Policy*, information practices and the *CAC* self-evaluation form to verify compliance with i-SAFE Harbor Guideline Requirements. If the Participant/Licensee's Web site is determined to be in full compliance with i-SAFE Harbor Guideline Requirements, it will then be listed as a Participant/Licensee in the i-SAFE Harbor program. i-SAFE Harbor Participant/Licensees are required to complete and submit an updated *CAC* self-evaluation form on an annual basis to ensure their Web site's information practices remain consistent with their posted *Privacy Policy* and i-SAFE Harbor Guideline Requirements.

C. Compliance Monitoring: i-SAFE Harbor Participant/Licensees must submit to monitoring reviews of their Web site's information practices. The purpose of monitoring reviews is to ensure that a Participant/Licensee's *Privacy Policy* is consistent with its Web site information practices. Monitoring reviews also allow i-SAFE to verify the Participant/Licensee's Web site complies with i-SAFE Harbor Guideline Requirements at all times. Compliance monitoring reviews (announced and/or unannounced) may be conducted quarterly or semi-annually or annually. If i-SAFE determines that a violation of i-SAFE Harbor Guideline Requirements has occurred, the Participant/Licensee is informed of the violation and also the corrective actions that must be taken to bring the Participant/Licensee's Web site into compliance. Failure to take corrective action(s) can result in a number of consequences, including removal from the i-SAFE Harbor program and referral to the appropriate governmental agency.

D. Consumer Complaints/Monitoring: i-SAFE Harbor Participant/Licensees must provide parents and children with reasonable and effective means to submit and attempt to resolve complaints about i-SAFE Harbor Participant/Licensee’s information practices (i.e., internal complaint/dispute resolution). i-SAFE Harbor also offers parents and children the opportunity to submit complaints about any i-SAFE Harbor Participant/Licensee directly to i-SAFE via third-party complaint/dispute resolution. In third-party complaint/dispute resolutions, an i-SAFE Harbor representative responds to all complaints immediately and i-SAFE Harbor Participant/Licensees must agree to work with i-SAFE representatives to cooperatively resolve all complaints submitted to i-SAFE Harbor for third-party complaint/dispute resolution. To support both Participant/Licensee internal complaint/dispute resolution processes and third-party complaint/dispute resolution processes, Participant/Licensees must maintain records for a period of three (3) years of all complaints, concerns or inquiries received about its Web site and any responses to consumers addressing such complaints or concerns.

E. License Agreement: i-SAFE Harbor Participant/Licensees must execute an i-SAFE Harbor Participant License Agreement (*PLA*). As part of this License Agreement, Participant/Licensees agree to comply with i-SAFE Harbor Guideline Requirements at all times. In the event a Participant/Licensee fails to meet any of its obligations under the *PLA*, such failure would constitute a material breach of the License Agreement and the i-SAFE Harbor Participant/Licensee’s membership in the i-SAFE Harbor program may be terminated.

F. Investigations/Referral to Governmental Agencies: In the event i-SAFE determines an i-SAFE Harbor Participant/Licensee has violated its posted *Privacy Policy* or any i-SAFE Harbor Guideline Requirements, i-SAFE may refer the Participant/Licensee to the Federal Trade Commission for possible unfair and deceptive trade practices.

I (D) Full Text of i-SAFE Harbor Guideline Requirements

See TAB 2

Part II: How i-SAFE Harbor Guideline Requirements, Assessment Mechanisms and Compliance Incentives Meet the Requirements of the Final Rule.

II (A) How i-SAFE Harbor Guideline Requirements Meet the Requirements of the Final Rule.

i-SAFE Harbor Guideline Requirements meet and exceed the requirements of §312.10 – safe harbors. i-SAFE Harbor Guideline Requirements were modeled on the principles of fair information practices of the Organization for Economic Co-Operation and Development (“OECD”), the Children’s Online Privacy Protection Act, and the requirements published in the Final Rule. In fact, i-SAFE Harbor Guideline Requirements were drafted to mirror §§312.2 through 312.9 of the Final Rule. Therefore, i-SAFE Harbor Participant/Licensees are assured that by implementing and complying with i-SAFE Harbor Guideline Requirements they are

providing the same or greater protections for children as those contained in the Final Rule. For example :

Section 312.2 (Defined Terms) - i-SAFE Harbor ensures all defined terms described in §312.2 of the Final Rule are adhered to because the Final Rule's definitions have been incorporated in i-SAFE Harbor Guideline Requirements. As a result, i-SAFE Harbor Participant/Licensees are required to read i-SAFE Harbor Guideline Requirements in a manner that is wholly consistent with §312.2 of the Final Rule.

Section 312.3 (General Requirements) - §312.3 of the Final Rule describes the overall scheme of the Children's Online Privacy Protection Act, which is to regulate unfair or deceptive acts or practices in connection with the collection , use and disclosure of personal information from and about children on the Internet. For example, §312.3 requires that a Web site operator must:

- Provide notice on the Web site or online service of what information it collects from children, how it uses such information, and disclosure practices for such information;
- Obtain verifiable parental consent prior to any collection, use and/or disclosure of personal information from children;
- Provide a reasonable means for a parent to review the personal the information collected from a child and to refuse to permit its further use or maintenance;
- Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity;
- Establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children.

All i-SAFE Harbor Participant/Licensees are required to adhere to and abide by this general requirement in order to prevent unfair or deceptive acts or practices in connection with the collection, use and/or disclosure of personal information from and about children 12 years old or younger on the Internet. Specifically, i-SAFE Harbor Participant/Licensees must comply with the following seven (7) Guideline Requirements [as noted in **Part I(C)** above]:

Requirement #1 (Notice/Disclosure of Information): i-SAFE Harbor Participant/Licensees must post a prominent link that is clearly labeled *Privacy Policy* or such similar notice that links parents or children to a description of the i-SAFE Harbor Participant/Licensee's information collection, use and/or disclosure practices.

Requirement #2 (Direct Notice to Parents): i-SAFE Harbor Participant/Licensees must make reasonable efforts to ensure parents of a child receive notice of the i-SAFE Harbor Participant/Licensee's information collection, use and/or disclosure practices with regard to children, including notice of any material change in the collection, use and/or disclosure practices to which the parent had previously consented.

Requirement #3 (Prior Verifiable Parental Consent): i-SAFE Harbor Participant/Licensees must obtain prior verifiable parental consent before any collection, use and/or disclosure of personal information from children unless permitted to collect a child's first name or online contact information under one of the exceptions to prior verifiable parental consent provided in §312.5(c) of the Final Rule.

Requirement #4 (Access and Review): i-SAFE Harbor Participant/Licensees must provide parents with the ability to access and review their child's personal information.

Requirement #5 (Restrictions on Information Collection): i-SAFE Harbor Participant/Licensees must not condition a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

Requirement #6 (Confidentiality, Security and Integrity Information): i-SAFE Harbor Participant/Licensees must establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children.

Requirement #7 (Compliance and Enforcement): i-SAFE Harbor Participant/Licensees must implement effective meaningful compliance and enforcement mechanisms that ensure they comply with their information *Privacy Policy* and practices.

Section 312.4 (Notice) – i-SAFE Harbor Guideline Requirements meet the requirement of §312.4 of the Final Rule that an operator of a Web site directed to children post a link to a notice of its information practices with regard to children on the homepage of its Web site and at each area on the Web site where personal information is collected from children. The notice of the i-SAFE Harbor Participant/Licensee's information practices must be clear and understandable and should not contain unrelated, contradictory or confusing material.

In particular, i-SAFE Harbor Guideline Requirements mandate that i-SAFE Harbor Participant/Licensees post a *Privacy Policy* that states: 1) the i-SAFE Harbor Participant/Licensee's contact information; 2) the types of personal information collected by the i-SAFE Harbor Participant/Licensee; 3) how the i-SAFE Harbor Participant/Licensee uses the personal information; 4) whether the i-SAFE Harbor Participant/Licensee discloses personal information it obtains from a child; 5) what form of control a parent or child has over their personal information; 6) any restrictions on information collection which i-SAFE Harbor Participant/Licensees must abide by when participating in the i-SAFE Harbor program; 7) how a parent or child can access and review their information; and 8) where a parent or child can submit a query or complaint to the i-SAFE Harbor Participant/Licensee about its Web site's information policies or practices.

i-SAFE Harbor Participant/Licensees must comply with the requirement for the size, location and operation of the *Privacy Policy* link on their Web site(s), which is described in the i-SAFE Harbor Guideline Requirements as follows:

“Clear and prominent place and manner” means that the link must stand out and be noticeable to the site's visitors through

use, for example, of a larger font size in a different color on a contrasting background. A link that is in small print at the bottom of the home page, or a link that is indistinguishable from a number of other, adjacent links is NOT “clear and prominent.”

Section 312.5 (Prior Verifiable Parental Consent) – i-SAFE Harbor Guideline Requirements meet the requirement of §312.5 of the Final Rule. i-SAFE Harbor Guideline Requirement #2 mandates that i-SAFE Harbor Participant/Licensees must obtain verifiable parental consent before any collection, use or disclosure of personal information from children. i-SAFE Harbor Participant/Licensees must also obtain such consent when there is any material change in the collection, use or disclosure practices to which the parent has previously consented.

Guideline Requirement #2 also circumscribes the appropriate methods that i-SAFE Harbor Participant/Licensees must use to obtain prior verifiable parental consent, which include the following:

1. WHEN PERSONAL INFORMATION OF A CHILD AGE 12 AND YOUNGER IS MADE PUBLICLY AVAILABLE the methods to obtain prior verifiable parental consent include: 1) providing a consent form to be signed by the parent and returned to the i-SAFE Harbor Participant/Licensee by postal mail or facsimile; 2) requiring the parent to use a credit card in connection with a transaction; 3) requiring the parent to send an e-mail containing the parent’s digital signature; 4) having a parent call a toll-free telephone number staffed by trained personnel; or 5) obtaining an e-mail with a PIN or password acquired through one of the four (4) verification methods above.

2. WHEN PERSONAL INFORMATION OF A CHILD AGE 12 AND YOUNGER IS USED ONLY FOR INTERNAL PURPOSES (i.e., the personal information will not be disclosed to third parties or made publicly available) the methods to obtain prior verifiable parental consent include the 5 methods listed in the preceding paragraph (#1. above) and also by the “email plus” method.² The “email plus” method allows Participant/Licensees to request (in the direct notice to parents) that the parent provide consent in an email message AND, after receiving the parent’s email consent, then confirming that it was, in fact, the parent who provided consent by taking the following additional (the “plus”) steps:

- Requesting in the Participant/Licensee’s initial email seeking consent that the parent include a phone or fax number or mailing address in the reply email, so that Participant/Licensees can follow up to confirm consent via telephone, fax, or postal mail; or
- After a reasonable time delay, sending another email to the parent to confirm consent. In this confirmatory email, Participant/Licensees should include all the original information contained in the direct notice, inform the parent that he or she can revoke the consent, and inform the parent how to revoke the consent.

² See footnote #1 regarding Participant/Licensee use of the “email plus” method.

GENERAL AUDIENCE AND TEEN WEB SITES: Although a Participant/Licensee may intend their Web site to be for adult and/or teen visitors/users, the need for verifiable parental consent always is triggered (i.e., *Section 312.5* of the Rule applies) when operators of general audience Web sites have actual knowledge that a particular visitor is a child. If an i-SAFE Harbor Participant/Licensee knows that a particular visitor to their Web site is a child, then the Rule must be followed with respect to that child. A Participant/Licensee can identify which visitors are ages 12 or younger, for example, by asking for age (or birth date) information at any point/place (on the site) where visitors/users can enter/provide personal information (i.e., “age-screen”). Participant/Licensees that choose to use age-screening to ensure personal information of children age 12 or younger is not collected, used or disclosed without prior verifiable parental consent should:

- Design age collection input screens in a manner that does not encourage children to provide a false age in order to gain access to the Participant/Licensee Web site;
- Ask age information in a neutral manner (e.g., a system that allows a user to freely enter month, day, and year of birth – but NOT just birth year and NOT a check box labeled “I am older than age 12”) at the point where the Web site invites visitors to provide personal information or to create a log-in user ID;
- Employ either temporary or permanent cookies to prevent children from “back-buttoning” to change their age in order to circumvent the requirement for verifiable parental consent or to obtain access to the site via, for example, an “entry point or gate.”
- Not encourage children to falsify their age information by stating, for example, that visitors age 12 or younger cannot participate on the Participant/Licensee Web site or should ask their parents before participating.

Upon entering age/birth date information that indicates the individual is a child age 12 or younger, an i-SAFE Harbor Participant/Licensee has several options, which include:

- Collecting the child’s parents’ contact information (e.g., email addresses) to provide direct notice and implement COPPA’s verifiable parental consent requirements; or,
- Configuring the Participant/Licensee data system to automatically delete personal information of visitors/users age 12 or younger, and direct them to content, if available, that does not involve collection or disclosure of personal information; or
- Considering whether the situation falls into one of the five (5) exceptions to the requirement of prior verifiable parental consent and act strictly in accord with the constraints of an applicable exception.

CHILDREN AND TEEN AUDIENCE WEB SITES: Where an i-SAFE Harbor Participant/Licensee Web site is directed to children and teens and does not age-screen, the i-SAFE Harbor Participant/Licensee must assume a site visitor is a child age 12 or younger and

obtain prior verifiable consent from the child's parent before collecting, using or disclosing the child's personal information.

Finally, even though prior verifiable parental consent is required under most situations before an i-SAFE Harbor Participant/Licensee is permitted to collect, use or disclose a child's personal information, there are a limited number exceptions in which an i-SAFE Harbor Participant/Licensee is permitted to collect a child's first name or online contact information before obtaining consent from the child's parent. In such circumstances, i-SAFE Harbor Participant/Licensees must comply with paragraph VII.A of Guideline Requirement #2, which describes the five (5) exceptions to prior verifiable parental consent and is consistent with §312.5(c) of the Final Rule.

Consistent with §312.5 of the Final Rule, i-SAFE Harbor Participant/Licensees also are required to give parents the option to consent to the collection and use of their child's personal information without consenting to disclosure of that information to third parties. **NOTE:** In the case of social networking sites, chat rooms, message boards and other similar online services, where sharing of personal information is part of the nature of such sites, the Rule does not require operators to give parents the choice to allow them to collect and use their children's personal information but not disclose it to third parties (i.e., because public disclosure of information is integral to such Web sites' operations). Therefore, i-SAFE Harbor Participant/Licensees who operate social networking sites, chat rooms, message boards and similar online services, must clearly disclose their Web sites' information collection and disclosure practices in their *privacy policy* and direct notice to parents so that parents understand their consent to collection equals consent to disclosure (i.e., because of the very nature of social networking sites, chat rooms, message boards, etc.) and can make an informed decision.

Section 312.6 (Right of Parent to Review Personal Information Provided by Child) – The i-SAFE Harbor Guideline Requirements meet the requirement of §312.6 of the Final Rule, which provides that upon the request of a parent whose child has provided personal information to a Web site the operator must provide the parent with an opportunity to access and review their child's personal information. In that regard, i-SAFE Harbor Guideline Requirements #3 and #4 mandate that i-SAFE Harbor Participant/Licensees provide parents with the ability to access and review their child's personal information AND that such parental access and review must consist of: 1) a description of the specific types of personal information collected from the child; 2) the opportunity at any time to refuse to permit the Participant/Licensee's further use or collection the child's personal information; and 3) the ability to direct the Participant/Licensee to delete the child's personal information from the Participant/Licensee's records.

Section 312.7 (Prohibition Against Conditioning A Child's Participation on Collection of Personal Information) – The i-SAFE Harbor Guideline Requirements meet the requirement of §312.7 of the Final Rule, which prohibits an operator of a Web site from conditioning a child's participation in a game, the offering of a prize, or other activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity. While i-SAFE recognizes that many Web sites may need (and require) a child to provide their personal information in order to participate in activities (e.g., games, contests or sweepstakes) on their Web site, and although the i-SAFE Harbor program does not limit such practices, i-SAFE Harbor Guideline Requirement #5 prohibits i-SAFE Harbor Participant/Licensees from conditioning a

child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity. In addition, i-SAFE Harbor Participant/Licensees also must continually re-evaluate whether a valid reason exists for the information to be collected. And, if the valid reason ceases to exist, i-SAFE Harbor Participant/Licensees must restrict their collection practices in view of their revised business practice/operation.

Section 312.8 (Confidentiality, Security, and Integrity of Personal Information Collected from Children) - The i-SAFE Harbor Guideline Requirements meet the requirement of §312.8 of the Final Rule by mandating that all i-SAFE Harbor Participant/Licensees establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children. i-SAFE Harbor Guideline Requirement #6, for example, mandates that i-SAFE Harbor Participant/Licensees must implement internal security measures that protect the confidentiality of the child's personal information and protect such information from loss, misuse, unauthorized access or improper disclosure.

Section 312.9 (Enforcement) - The i-SAFE Harbor program's compliance and enforcement mechanisms meet the requirements of §312.9 of the Final Rule in that i-SAFE Harbor Participant/Licensees are required to implement internal control mechanisms, including but not limited to appointing a representative ("program representative") of the i-SAFE Harbor Participant/Licensee that is responsible for handling all questions or complaints received from parents or children that use its Web site. Program representatives must be given full authority to receive and actively respond to any privacy related inquiries. In the event an i-SAFE Harbor Participant/Licensee has not adequately responded to a parent or child's inquiry, the i-SAFE Harbor Participant/Licensee must provide a means for the parent or child to appeal to a higher management level. Moreover, if a parent or child remains unsatisfied with the i-SAFE Harbor Participant/Licensee's response, the i-SAFE Harbor Participant/Licensee is required to refer the parent or child to i-SAFE Harbor representatives.

In addition to these internal control mechanisms, i-SAFE Harbor also requires i-SAFE Harbor Participant/Licensees to adhere to i-SAFE Harbor Guideline Requirement #7 "Compliance Enforcement and Complaint/Dispute Resolution." i-SAFE Harbor Participant/Licensees agree [contractually via the terms and conditions in the Participant License Agreement (*PLA*)] to submit to compliance enforcement mechanisms (e.g., monitoring reviews) and to cooperate in all respects with the i-SAFE Harbor complaint/dispute resolution process. For example: The *PLA* states in part at paragraph VIII.B that:

"Licensee agrees to fully comply with and participate in, without any limitations or conditions or restrictions, i-SAFE Harbor Guideline Requirements, including the requirements for self-assessments and independent assessments, compliance monitoring reviews and the proceedings associated with the compliance enforcement Complaint/Dispute Resolution Process."

Moreover, i-SAFE Harbor Participant/Licensees must provide parents and children with reasonable and effective means to submit complaints about i-SAFE Harbor

Participant/Licensee's information practices. i-SAFE Harbor's compliance enforcement mechanisms are discussed in further detail below.

II (B) How i-SAFE Harbor Assessment Mechanisms Required Under §312.10(b)(2) Provide Effective Enforcement of the Requirements of the Final Rule.

Mandatory mechanism for independent assessment of an operator's compliance with the guidelines. i-SAFE Harbor (including its self-assessment and independent assessment mechanisms) meets the requirements of §312.10(b)(2) of the Final Rule. Section 312.10(b)(2) states that an effective, mandatory mechanism for the independent assessment of an i-SAFE Harbor Participant/Licensee's compliance with the i-SAFE Harbor Guideline Requirements is required. i-SAFE Harbor accomplishes this requirement in a number of ways, including the following:

Initial Self-Assessments - Using the i-SAFE Harbor Compliance Assessment Checklist (***CAC***), applicants to become i-SAFE Harbor Participant/Licensees must conduct an initial self-assessment of their Web site information collection, use and disclosure practices. Each applicant is required to attest to the accuracy of the statements they make on the ***CAC*** concerning their information practices.

Upon submission of an applicant's initial ***CAC*** to the i-SAFE Harbor program, prospective i-SAFE Harbor Participant/Licensees must then successfully pass an initial Qualification Audit Review (***QAR***), which is conducted independently by i-SAFE Harbor personnel. During the initial ***QAR***, i-SAFE Harbor representatives:

1. Determine whether or not the prospective Participant/Licensee's privacy statement is an accurate representation of its internal and external information practices;
2. Ensure the prospective Participant/Licensee's information practices meet all i-SAFE Harbor Guideline Requirements; and
3. Assess the likelihood that the prospective Participant/Licensee will continue to meet the i-SAFE Harbor Guideline Requirements on a consistent basis.

During the initial ***QAR***, i-SAFE Harbor compares the responses made by the prospective i-SAFE Harbor Participant/Licensee in its ***CAC*** with the notice and disclosure statements contained in the posted ***Privacy Policy***. Any inaccuracies noted in the applicant's ***Privacy Policy*** must be modified to accurately reflect the applicant's actual information practices before the i-SAFE Harbor will execute a Participant License Agreement (***PLA***) and authorize the display of the i-SAFE Harbor emblem on the i-SAFE Harbor Participant/Licensee's Web site.

The next step in the initial ***QAR*** process includes a trained information privacy monitor's review of the applicant's Web site and comparison of the Web site review with the applicant's ***CAC*** and posted ***Privacy Policy*** to ensure the ***Privacy Policy*** accurately depicts the collection practices of the Web site.

The next step in the initial **QAR** process involves a trained information privacy monitor reviewing the applicant's Web site collection and use practices. During this segment of the Web site review process, the information privacy monitor will submit fictitious information at each point within the Web site where information is collected and investigate (i.e., attempt to confirm) whether or not the prospective i-SAFE Harbor Participant/Licensee is properly collecting contact information or personal information in conformity with the Rule and their stated *Privacy Policy*. If the information privacy monitor detects that personal information is collected from children age 12 or younger, the monitor then confirms (i.e., via the results of the "seeded" fictitious information) whether or not prior verifiable parent consent is obtained before the child's personal information is collected by the Web site.

When an applicant's Web site is determined to be in full compliance with i-SAFE Harbor Guideline Requirements and the applicant has executed a **PLA**, it will be listed online as an i-SAFE Harbor Participant/Licensee. To ensure i-SAFE Harbor Participant/Licensees remain in good standing and full compliance with i-SAFE Harbor Guideline Requirements, each Participant/Licensee must submit to the procedures described above on an annual basis. This allows i-SAFE Harbor to make sure the Participant/Licensee's Web site is in full compliance with i-SAFE Harbor Guideline Requirements and COPPA before renewing the Web site's participation/license in the i-SAFE Harbor program for an additional year.

Annual Self-Assessments – i-SAFE Harbor Guideline Requirements and the Participant License Agreement (**PLA**) mandate that i-SAFE Harbor Participant/Licensees annually perform a self-assessment [using the i-SAFE Harbor Compliance Assessment Checklist (**CAC**)] of their Web site *Privacy Policy* and information collection, use and disclosure policies and practices.

Periodic Monitoring - i-SAFE Harbor Participant/Licensees must submit to periodic announced and/or unannounced monitoring reviews (i.e., independent assessments) of their Web site's information policies and practices. The purpose of these independent monitoring reviews is to ensure that an i-SAFE Harbor Participant/Licensee's *Privacy Policy* is, and remains, consistent with its extant Web site's information practices. Periodic monitoring also allows i-SAFE Harbor to verify that the i-SAFE Harbor Participant/Licensee's Web site complies with the i-SAFE Harbor Guideline Requirements and COPPA at all times.

All i-SAFE Harbor Participant/Licensees must submit to independent periodic monitoring reviews of their Web site's information practices. Periodic monitoring will be accomplished at least twice a year and as much as four times per year. Periodic monitoring is conducted by trained i-SAFE personnel who systematically navigate throughout an i-SAFE Harbor Participant/Licensee's Web site for the purpose of ensuring: 1) there is prominent link to the i-SAFE Harbor Participant/Licensee's Web site's *Privacy Policy* on the homepage and any Web page where information is collected by the Web site; 2) the i-SAFE Harbor Participant/Licensee obtains prior verifiable parental consent from all children 12 years old and younger before collecting their personal information; and 3) the i-SAFE Harbor Participant/Licensee's Web site continually remains in full compliance with i-SAFE Harbor Guideline Requirements. During periodic monitoring, i-SAFE Harbor also will, from time-to-time, "seed" personal information the i-SAFE Harbor Participant/Licensee Web site has collected. During this process, the information privacy monitor submits fictitious information

into the i-SAFE Harbor Participant/Licensee's Web site database to track how Participant/Licensee uses the fictitious personal information collected/seeded. These periodic monitoring reviews are an additional compliance enforcement mechanism by which i-SAFE Harbor can ensure that i-SAFE Harbor Participant/Licensees are adhering to their Web site's posted *Privacy Policy*.

Periodic monitoring reviews are memorialized in written reports and maintained by i-SAFE Harbor for a period of three (3) years.

Consumer Complaints/Monitoring – i-SAFE Harbor Participant/Licensees must provide parents and children with reasonable and effective means to submit complaints about i-SAFE Harbor Participant/Licensee's information practices. i-SAFE Harbor also offers the parents and/or children the opportunity to submit complaints about i-SAFE Harbor Participant/Licensees directly to i-SAFE Harbor representatives, who will respond to all complaints immediately.

II (C) How i-SAFE Harbor Compliance Incentives Required Under §312.10(b)(3) Provide Effective Enforcement of the Requirements of the Final Rule.

Effective incentives for subject operator's compliance with the Guidelines. Section 312.10(b)(3) of the Final Rule requires i-SAFE Harbor to provide effective incentives that will ensure i-SAFE Harbor Participant/Licensee's full compliance with i-SAFE Harbor Guideline Requirements. This Final Rule requirement is met in the following manner:

Participant License Agreement Obligations - i-SAFE Harbor Participant/Licensees must execute an i-SAFE Harbor Participant License Agreement (***PLA***). In the ***PLA***, i-SAFE Harbor Participant/Licensees agree to comply with i-SAFE Harbor Guideline Requirements at all times. In the event an i-SAFE Harbor Participant/Licensee fails to meet any of its ***PLA*** obligations, such failure(s) would constitute a material breach of the ***PLA*** and the Participant/Licensee's participation in the i-SAFE Harbor program may be suspended and/or terminated.

Consumer Complaint/Dispute Resolution – i-SAFE Harbor Participant/Licensees are required to implement effective and affordable mechanisms that ensure compliance with its *Privacy Policy* and provide appropriate means of resolving consumer complaints/disputes. Mechanisms for resolving consumer complaints/disputes include the appointment of at least one individual (i.e., "program representative") to whom parents and/or children can submit queries or complaints about i-SAFE Harbor Participant/Licensee's privacy practices. Program representatives must be given the authority by their respective i-SAFE Harbor Participant/Licensees to investigate all queries, complaints or disputes and complete an investigation in a timely manner.

i-SAFE Harbor Participant/Licensees are required to cooperate with i-SAFE Harbor's efforts to resolve queries, complaints and disputes. In the event a parent or child is not satisfied with the response/resolution provided by an i-SAFE Harbor Participant/Licensee, the i-SAFE Harbor Participant/Licensee is required to refer the parent or child to an i-SAFE Harbor representative.

Any time i-SAFE Harbor determines an i-SAFE Harbor Participant/Licensee has violated i-SAFE Harbor Guideline Requirements, the i-SAFE Harbor Participant/Licensee is informed of violation and the corrective actions it must take to bring the Participant/Licensee's Web site into compliance. Failure to take corrective action(s) can result in various consequences, including termination from the i-SAFE Harbor program (as described in the paragraph above regarding "Participant Licensee Agreement Obligations") and referral to the appropriate governmental agency (as described in the "Referral to the Commission" paragraph below).

i-SAFE Harbor Participant/Licensees must maintain records for three (3) years of all consumer queries and complaints/disputes and the Participant/Licensee's investigations and resolutions and referrals.

Referral to the Commission – When, after thorough investigation of an i-SAFE Harbor Participant/Licensee's information practices, i-SAFE Harbor makes a determination that the Participant/Licensee has violated its posted *Privacy Policy* and/or i-SAFE Harbor Guideline Requirements, i-SAFE Harbor may, at its sole discretion, refer the matter to the Federal Trade Commission as a possible unfair and deceptive trade practice.

Part III: Comparison of each provision of §§312.3 through 312.8 of the Final Rule with the corresponding provisions of i-SAFE Harbor Guideline Requirements.

See chart at TAB 3

Part IV: Conclusion

i-SAFE respectfully submits this application for safe harbor status to the Commission for the purpose of demonstrating i-SAFE Harbor meets all the requirements of the Final Rule. We believe i-SAFE Harbor program elements (i.e., Guideline Requirements, Compliance Assessment Checklist, Qualification Audit Review, Participant License Agreement, Periodic Monitoring Reviews, and Internal and Third Party Complaint/Dispute Resolution Process) will provide an effective self-regulatory program for protecting the personal information of children online and involving parents in the process.