

**BY COMPLETING THIS SUPPLEMENTAL APPLICATION THE APPLICANT IS APPLYING FOR COVERAGE WITH FEDERAL INSURANCE COMPANY (THE "COMPANY")**

**NOTICE: THE LIABILITY COVERAGE PARTS PROVIDE CLAIMS MADE COVERAGE, WHICH APPLIES ONLY TO "CLAIMS" FIRST MADE DURING THE "POLICY PERIOD", OR ANY APPLICABLE EXTENDED REPORTING PERIOD. THE LIMIT OF LIABILITY TO PAY DAMAGES OR SETTLEMENTS WILL BE REDUCED AND MAY BE EXHAUSTED BY "DEFENSE COSTS", AND "DEFENSE COSTS" WILL BE APPLIED AGAINST THE RETENTION. IN NO EVENT WILL THE COMPANY BE LIABLE FOR "DEFENSE COSTS" OR THE AMOUNT OF ANY JUDGMENT OR SETTLEMENT IN EXCESS OF THE APPLICABLE LIMIT OF LIABILITY. READ THE ENTIRE NEW BUSINESS APPLICATION CAREFULLY BEFORE SIGNING.**

**SUPPLEMENTAL APPLICATION INSTRUCTIONS:**

1. Whenever used in this Supplemental Application, the term "**Applicant**" shall mean the parent organization and all subsidiaries, unless otherwise stated.
2. Please attach the following for the requested coverages as indicated below:

Partnerships:

- (a) The most recently amended partnership agreement(s) for each applicable organization.
- (b) An organization chart, including ownership percentage of all partner owners.

Employed Lawyers Liability Coverage: Most recent annual financial statements, audited if outside audits are performed.

CyberSecurity Coverage: Risk assessment of the **Applicant** performed by an organization other than the **Applicant**;

3. In addition to the relevant sections of the New Business Application, the **Applicant** must complete each section of the Supplemental New Business Application that corresponds with the optional coverage for which the **Applicant** desires a proposal and sign and date this Supplemental New Business Application.
4. If either Employed Lawyers Liability or CyberSecurity coverage is being requested and are not currently purchased, or if the Applicant is requesting larger limits than are currently purchased, as indicated in Section II, Insurance Information, of the New Business Application, the Applicant must complete Section V, Warranty, of the New Business Application.

I. **NAME OF APPLICANT:** \_\_\_\_\_

II. **ADDITIONAL RISK INFORMATION FOR PARTNERSHIPS:**

If the **Applicant's** organization is formed as a partnership or limited partnership, or if it or any of its subsidiaries act as a general partner for another organization, please answer the following:

1. Nature of the partnership(s)' business, if different than **Applicant**: \_\_\_\_\_
2. Indicate type of partnership:
 

(a) Limited Partnership (LP)	<input type="checkbox"/> Yes <input type="checkbox"/> No
(b) Limited Liability Partnership (LLP)	<input type="checkbox"/> Yes <input type="checkbox"/> No
(c) Limited Liability Limited Partnership (LLLLP)	<input type="checkbox"/> Yes <input type="checkbox"/> No
(d) General Partnership	<input type="checkbox"/> Yes <input type="checkbox"/> No
(e) Other (please specify): _____	
3. If this organization is formed as a limited partnership:
  - (a) List the name of the general partner: \_\_\_\_\_
  - (b) Indicate the percentage ownership the general partner has in the limited partnership:  
\_\_\_\_\_ %
4. Does the Applicant have a mandatory retirement policy?  Yes  No  
If "Yes", please attach details.

**III. COVERAGE SPECIFIC INFORMATION:**

**A. EMPLOYED LAWYERS LIABILITY (APPLICANT: *Please complete only if requesting this coverage*)**

1. Provide the total number of attorneys as follows:

- (a) Employed Lawyers: \_\_\_\_\_
- (b) Temporary Attorneys: \_\_\_\_\_
- (c) Contract Attorneys: \_\_\_\_\_ (Not including outside legal counsel)
- (d) Employed Lawyers with more than ten (10) years of legal experience: \_\_\_\_\_
- (e) Employed Lawyers that are members of the Association of Corporate Counsel: \_\_\_\_\_

2. Do any Employed Lawyers, Temporary Attorneys or Contract Attorneys provide legal services in any of the following practice areas:

- (a) Environmental Law & Compliance  Yes  No
- (b) Copyright, Patent, Trademark and Other Intellectual Property Law  Yes  No
- (c) Litigation  Yes  No
- (d) Securities Law  Yes  No

3. Describe the types of legal work typically referred by the **Applicant** to outside counsel:

\_\_\_\_\_

4. Do any Employed Lawyers provide Moonlighting Legal Services?  Yes  No

If "Yes", describe the scope of services provided and the total number of hours annually.

\_\_\_\_\_

5. Has any person proposed for this coverage been the subject of, or been involved in, any of the following arising out of his or her provision of legal services, irrespective of whether such activity arose out of work performed for the **Applicant**:

- (a) Any reprimand, sanction, fine or discipline by, or refused admission to, a bar association, court, administrative or regulatory agency?  Yes  No
- (b) Any civil or criminal litigation, arbitration, claim or administrative or regulatory proceeding during the last five years?  Yes  No

**B. CYBERSECURITY (APPLICANT: *Please complete only if requesting this coverage. Note, CyberSecurity includes a Liability Coverage Part.*)**

1. Does the **Applicant** anticipate in the next twelve months establishing or entering into any related or unrelated ventures which are a material change in operations?  Yes  No

If "Yes", please provide full details on a separate sheet.

2. Please indicate the **Applicant's** GROSS annual revenue from on-line sales or services:

\_\_\_\_\_

3. How many servers does the **Applicant** either own or otherwise have dedicated to their use?

\_\_\_\_\_

4. What is the **Applicant's** total number of IP addresses? \_\_\_\_\_

5. Does the **Applicant** collect, store or process personally identifiable, Protected Health Information(PHI) or other confidential information?  Yes  No

(a) If "Yes", is it encrypted?  Yes  No

(b) If "Yes", how many records are held, including the **Applicant's** prospective, current and former customers and employees? \_\_\_\_\_

6. Is the **Applicant** subject to any of the following:

(a) HIPAA Privacy and Security  Yes  No

(b) The Payment Card Industry (PCI) Security Standard?  Yes  No

If "Yes", complete PCI Compliance section of this Application.

(c) The Gramm, Leach, Bliley Act?  Yes  No

(d) Red Flags Rule?  Yes  No

(e) Any other federal or state law or regulation concerning privacy or the safeguarding of personally identifiable or other confidential information (other than state "breach notification" laws)?  Yes  No

If "Yes", please indicate what law(s) or regulation(s): \_\_\_\_\_

If "Yes", to any of the above in Question 6, is the **Applicant** compliant with the selected rules and standards?  Yes  No

If "No", please explain the **Applicant's** lack of compliance: \_\_\_\_\_

7. Does the **Applicant** process or store personally identifiable, Protected Health Information (PHI) or other confidential information for third parties and is encrypted?  Yes  No

If "Yes", please attach an explanation.

8. Does the **Applicant** shred all written or printed personally identifiable, Protected Health Information (PHI) or other confidential information when it is being discarded?  Yes  No

**HIPAA COMPLIANCE**

1. Is the **Applicant** a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA), HITECH, or any applicable state law?  Yes  No

2. Is the **Applicant** a Business Associate under any of the laws in Question 1.  Yes  No

(a) If "Yes" to 1 or 2 above, approximately how many individuals' protected health information (PHI) does the **Applicant** collect, store or process?  
\_\_\_\_\_

(b) If "Yes" to 1 or 2 above, is the **Applicant** in full compliance with the provisions of any applicable law(s) outlined in Question 1?  Yes  No

If the **Applicant** is not in full compliance with any of the applicable law(s) in Question 1, when will the **Applicant** be in full compliance?  
\_\_\_\_\_

3. (a) Has the **Applicant** been audited by The Department of Health and Human Services (HHS), or any other agency under the authority of HHS, for their compliance with the either the HIPAA Privacy Rule or Security Rule?  Yes  No

(b) If "Yes" to 3(a), was the **Applicant** found to be in compliance?  Yes  No

(c) If "No" to 3(a), please indicate in which areas the **Applicant** was found not to be in compliance: \_\_\_\_\_

(d) If "No" to 3(a), have all areas of non-compliance been rectified?  Yes  No

4. Does the **Applicant** conduct regular audits of their HIPAA Privacy and Security controls and procedures?  Yes  No

5. Does the **Applicant** remediate any areas in which they are found not to be in compliance within:
- (a) 30 days;  Yes  No
  - (b) 90 days;  Yes  No
  - (c) 180 days;  Yes  No
  - (d) more than 180 days.  Yes  No
6. In the **Applicant's** contracts with any of their Business Associates does the **Applicant** require that the business associates indemnify the **Applicant** for any liability the **Applicant** incurs as a result of the business associates' non-compliance with HIPAA, the HITECH Act or any failure or alleged failure to keep the **Applicant's** information secure?  Yes  No

**WRITTEN RECORDS MANAGEMENT**

1. Does the **Applicant** collect sensitive information through hand written applications, forms or notes?  Yes  No
- If "Yes", does the **Applicant** shred such documents after entering the information into their computer system?  Yes  No
- If "No", does the **Applicant**:
- (a) Retain the documents in secured encrypted files?  Yes  No
  - (b) Store such documents in secure areas that minimize access by persons not authorized to view such documents?  Yes  No
  - (c) Enforce a clean desk policy?  Yes  No
  - (d) Shred such documents when they are ultimately disposed of?  Yes  No
2. Is sensitive information in *any written form* (handwritten, typed, or printed) stored with a third party?  Yes  No
- (a) If "Yes" to 2:
    - i) Does the **Applicant** have a written contract with the respective service provider(s) or vendor(s)?  Yes  No
    - ii) Are third party service provider(s) or vendor(s) required to have or do they have E&O or Cyber Insurance to respond to a breach?  Yes  No

If "No", please attach an explanation.
  - (b) If "Yes" to 2, does the **Applicant's** contract with the service provider(s) state that the service provider:
    - i) Has primary responsibility for the security of the **Applicant's** information?  Yes  No
    - ii) Has a contractual responsibility to indemnify the **Applicant** for any loss or expenses associated with any failure to safeguard the **Applicant's** electronic data?  Yes  No
  - (c) If "Yes" to 2, does the **Applicant** review their most recent information security audit (i.e. SAS 70)?  Yes  No
- If "No", please attach an explanation.

**PCI Compliance**

*(Please answer the questions in this section if the Applicant is subject to the PCI Security Standard)*

1. How many credit or debit card transactions does the **Applicant** process annually? \_\_\_\_\_
2. Does the **Applicant**:

- (a) Mask all but the last four digits of a card number when displaying or printing cardholder data?  Yes  No
- (b) Ensure that card-validation codes are not stored in any of the **Applicant's** databases, log files or anywhere else within their network?  Yes  No
- (c) Encrypt all account information on the **Applicant's** databases?  Yes  No
- (d) Encrypt or use tokenization for all account information at the point of sale?  Yes  No

**Information Security Policies**

- 1. Has the **Applicant** implemented a formal information security policy which is applicable to all of the **Applicant's** business units?  Yes  No  
If "Yes",
  - (a) Does the **Applicant** test the security required by the security policy at least annually?  Yes  No
  - (b) Does the **Applicant** regularly identify and assess new threats and adjust the security policy to address the new threats?  Yes  No
  - (c) Does the **Applicant's** information security policy include policies for the use and storage of personally identifiable or other confidential information on laptops?  Yes  No

**Web Server Security**

- 1. Does the **Applicant** store personally identifiable or other confidential information on their web servers?  Yes  No
- 2. Do the **Applicant's** web servers have direct access to personally identifiable or other confidential information?  Yes  No
- 3. Does the **Applicant** have firewalls that filter both inbound and outbound traffic?  Yes  No

**Virus Prevention, Intrusion Detection & Penetration Testing**

- 1. Are anti-virus programs installed on all of the **Applicant's** PC's and network systems?  Yes  No  
If "Yes", how frequently are the virus detection signatures updated?  
\_\_\_\_\_
- 2. Does the **Applicant** employ intrusion detection or intrusion protection devices on their network, or IDS or IPS software on the **Applicant's** hosts?  Yes  No  
If "Yes", how frequently are logs reviewed? \_\_\_\_\_
- 3. Does the **Applicant** run penetration tests against all parts of their network?  Yes  No  
If "Yes", how often are the tests run? \_\_\_\_\_
- 4. Has the **Applicant** been the target of any computer or network attacks (including virus attacks) in the past two (2) years?  Yes  No  
If "Yes", did the number of attacks increase?  Yes  No

**Mobile Device Security**

- 1. Does the **Applicant** store personally identifiable, Protected Health Information (PHI) or other confidential information on mobile devices?  Yes  No  
If "Yes", does the **Applicant** encrypt such information?  Yes  No

**Business Continuity**

- 1. Does the **Applicant** have a Business Continuity Plan [BCP] specifically designed to address a network related denial-of-service attack?  Yes  No  
If "Yes":

- (a) Is the BCP reviewed and updated at least bi-annually?  Yes  No
- (b) Is the BCP tested at least annually?  Yes  No
- (c) Have any problems been rectified?  Yes  No

**Security Assessments**

- 1. Has an external system security assessment, other than vulnerability scans or penetration tests, been conducted within the past twelve (12) months?  Yes  No

If "Yes", please indicate who conducted the assessment, attach copies of the results, and indicate whether all critical recommendations have been corrected or complied with.

If "No", please attach explanation.

**Backup & Archiving**

- 1. How frequently does the **Applicant** back up electronic data? \_\_\_\_\_
- 2. Does the **Applicant** store back up electronic data with a third party service provider?  Yes  No

- (a) If "Yes",
  - i) Does the **Applicant** have a written contract with the respective service provider(s) or vendor(s)?  Yes  No
  - ii) Are third party service provider(s) or vendor(s) that store back up electronic data required to have or do they have E&O or Cyber Insurance to respond to a breach?  Yes  No

If "No", please attach an explanation.

- (b) If "Yes" to 2(a)(i), does the **Applicant's** contract with the service provider(s) state that the service provider:
  - i) Has primary responsibility for the security of the **Applicant's** information?  Yes  No
  - ii) Has a contractual responsibility to indemnify the **Applicant** for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data?  Yes  No

- (c) If "Yes" to 2, does the **Applicant** review their most recent information security audit (i.e. SAS70)?  Yes  No

If "No", please attach an explanation.

**Service Providers**

- 1. Does the **Applicant** use third party technology service providers?  Yes  No
- a) If "Yes",

- i) Does the **Applicant** have a written contract with the respective service provider(s) or vendor(s)?  Yes  No
- ii) Are third party service provider(s) or vendor(s) required to have or do they have E&O or Cyber Insurance to respond to a breach?  Yes  No

If "No", please attach an explanation.

- (b) If "Yes" to 1(a)(i), does the **Applicant's** contract with the service provider(s) state that the service provider:
  - i) Has primary responsibility for the security of the **Applicant's** information?  Yes  No
  - ii) Has a contractual responsibility to indemnify the **Applicant** for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data?  Yes  No

- (c) If "Yes" to 1, does the **Applicant** review their most recent information security audit (i.e. SAS70)?  Yes  No

If "No", please attach an explanation.

**Incident Response Plans**

- 1. Does the **Applicant** have a formal incident response plan that addresses network security incidents or threats?  Yes  No

**Security Incident And Loss History:**

- 1. Has the **Applicant** had any computer or network security incidents during the past two years? Incident includes any unauthorized access or exceeding authorized access to any computer, system, data base or data; intrusion or attack; the denial of use of any computer or system; intentional disruption, corruption or destruction of electronic data, programs or applications; or any other incidents similar to the foregoing?  Yes  No

*Note: if the answer to this Question 1 is "Yes", please attach a complete description of the incident(s), including whether the **Applicant** reported the incident(s) to law enforcement and/or the **Applicant's** insurance carrier.*

**C. WORKPLACE VIOLENCE EXPENSE (APPLICANT: Please complete only if requesting this coverage)**

- 1. Total number of locations: \_\_\_\_\_
- 2. Does the **Applicant** have:
  - (a) An Employee Assistance Program (EAP)?  Yes  No
  - (b) A progressive discipline policy?  Yes  No
  - (c) An employee complaint/grievance resolution procedure?  Yes  No
  - (d) A customer complaint/grievance resolution procedure?  Yes  No
  - (e) A written policy on workplace violence that is circulated to all employees?  Yes  No
  - (f) A program to train supervisory and management employees to recognize, report and respond to potentially hostile employees or situations?  Yes  No
  - (g) A process for performing background checks for potential employees?  Yes  No

If "Yes," please explain:

\_\_\_\_\_

- 3. What security precautions does the **Applicant** have in place to limit access to its premises from hostile or volatile persons?

\_\_\_\_\_

**Workplace Violence Loss Experience**

- 4. List all workplace violence incidents discovered by the **Applicant** in the last three years, itemizing each incident separately. Include date of loss, description and total amount of loss. (Attach additional pages if necessary.) Check if none:

\_\_\_\_\_

\_\_\_\_\_

**IV. MATERIAL CHANGE:**

If there is any material change in the answers to the questions in this Supplemental Application before the policy inception date, the **Applicant** must immediately notify the Company in writing, and any outstanding quotation may be modified or withdrawn.

**V. DECLARATIONS, FRAUD WARNINGS AND SIGNATURES:**

The **Applicant's** submission of this Supplemental Application does not obligate the Company to issue, or the **Applicant** to purchase, a policy. The **Applicant** will be advised if the Supplemental Application for coverage is accepted. The **Applicant** hereby authorizes the Company to make any inquiry in connection with this Supplemental Application.

The undersigned authorized agents of the person(s) and entity(ies) proposed for this insurance declare that to the best of their knowledge and belief, after reasonable inquiry, the statements made in this Supplemental Application and in any attachments or other documents submitted with this Supplemental Application are true and complete. The undersigned agree that this Supplemental Application and such attachments and other documents shall be the basis of the insurance policy should a policy providing the requested coverage be issued; that all such materials shall be deemed to be attached to and shall form a part of any such policy; and that the Company will have relied on all such materials in issuing any such policy.

The information requested in this Supplemental Application is for underwriting purposes only and does not constitute notice to the Company under any policy of a Claim or potential Claim.

**Notice to Alabama and Maryland Applicants:** Any person who knowingly and willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly and willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

**Notice to Arkansas, New Mexico and Ohio Applicants:** Any person who, with intent to defraud or knowing that he/she is facilitating a fraud against an insurer, submits an application or files a claim containing a false, fraudulent or deceptive statement is, or may be found to be, guilty of insurance fraud, which is a crime, and may be subject to civil fines and criminal penalties.

**Notice to Colorado Applicants:** It is unlawful to knowingly provide false, incomplete or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policy holder or claimant for the purpose of defrauding or attempting to defraud the policy holder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory agencies.

**Notice to District of Columbia Applicants:** WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits, if false information materially related to a claim was provided by the applicant.

**Notice to Florida Applicants:** Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

**Notice to Kentucky Applicants:** Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime.

**Notice to Louisiana and Rhode Island Applicants:** Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

**Notice to Maine, Tennessee, Virginia and Washington Applicants:** It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines or a denial of insurance benefits.

**Notice to New Jersey Applicants:** Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

**Notice to Oklahoma Applicants:** WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

**Notice to Oregon and Texas Applicants:** Any person who makes an intentional misstatement that is material to the risk may be found guilty of insurance fraud by a court of law.

**Notice to Pennsylvania Applicants:** Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.



**Notice to Puerto Rico Applicants:** Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand (5,000) dollars and not more than ten thousand (10,000) dollars, or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances are present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

**Notice to New York Applicants:** Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and shall also be subject to: a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

**SIGNATURE OF APPLICANT'S AUTHORIZED REPRESENTATIVE**

Date

Signature\*

Title

\_\_\_\_\_

\*This Supplemental Application must be signed by the chief executive officer, president or chief financial officer of the **Applicant's** parent organization acting as the authorized representative(s) of the person(s) and entity(ies) proposed for this insurance.

<u>Produced By:</u>		
Agent: _____		
Agency: _____		
Agency Taxpayer ID or SS No.: _____	Agent License No.: _____	
Address: _____		
City: _____	State: _____	Zip: _____
<u>Submitted By:</u>		
Agency: _____		
Agency Taxpayer ID or SS No.: _____		
Agent License No.: _____		
Address: _____		
City: _____	State: _____	Zip: _____