AIG GLOBAL VENDOR CERTIFICATION POLICY

Global Security

AIG VENDOR CERTIFICATION POLICY

1. Purpose

American International Group, Inc. and its member companies, subsidiaries, and its affiliates (collectively, "AIG" or "we" or "our") have developed mutually beneficial relationships with our vendors, consultants, and contractors – relationships built on mutual trust and pride in the services we provide to our customers. Experience has proven that the vast majority of our vendors, consultants, and contractors are highly qualified and reputable. The background screening program described in this policy ("AIG Vendor Certification Program") is established to ensure that those standards are met and adhered to by all AIG vendors (each, a "Vendor") and their personnel (such employees and contractors, collectively, "Workers") who require Access (as defined below) and their subcontractors that require Access. All references to "Vendor" in this policy shall be deemed to refer to any such subcontractor, and all references to "Workers" in this policy shall be deemed to refer to any such subcontractor's personnel. In the event that this policy is included in an agreement between AIG and a Vendor, all capitalized terms defined in this policy shall be applicable only to this policy.

2. Scope

The terms of this policy apply globally with respect to all Vendors and Workers. AIG Global Security, in conjunction with a third party vendor performing background screening for AIG ("Screening Provider"), administers the AIG Vendor Certification Program.

3. Requirements

The following requirements are applicable to the AIG Vendor Certification Program:

- The AIG Vendor Certification Program applies to all Vendors and Workers requiring any of the following ("Access"):
  - Routine unescorted access to AIG facilities (owned or leased).
  - Any access to AIG systems, networks, or applications.
  - Any access to AIG confidential information (i.e., AIG information other than information that AIG makes publicly available), regardless of the time period or location, to include any form of remote access or manner that AIG information / data is received.

- Labor union workers are not exempt from compliance with the AIG Vendor Certification Program.

- Vendor and Workers must complete all forms for certification and AIG Global Security must

approve the certification before the Vendor and Workers may provide services to AIG.

4. Background Screening Process/Steps

The following steps and procedures are required elements in the process of obtaining background screenings for potential Vendors and their Workers, as permitted by local laws:

4.1 Vendor Screening

- Vendors and their Workers must visit the website designated by AIG (currently www.aigscreen.com/kiosk) to prepare and submit their applications and all appropriate consent forms. The Worker screening will be conducted as outlined in Section 4.3.

KEY POINTS:

- Publicly traded companies are exempt from an AIG background check due to being subjected to a stringent governmental review prior to their stock exchange listing. Privately held companies are required to undergo background checks.

- Workers (whether working for a publicly traded company or not) who require Access will be subject to the screening process, except to the extent that Vendor (i.e., the company itself) has been approved to use its own background check process in accordance with the Validated Third Party Program (see Section 4.2).

- AIG background checks on Workers are valid for five (5) years. After the five (5) year time period expires, a new background check will be initiated. This new check will be limited to the prior five (5) years or the time period since the completion of the previous background check. Vendors are responsible for managing and auditing the life cycle of background checks for their Workers and prior to the expiration will be required to initiate a new background check request. **REMINDER: New Vendors (and their Workers) are NOT authorized to begin work until their background checks have returned approved.**

- In the event that any background check (or certain elements thereof) would violate local laws, regulations or practices, AIG and Vendor shall discuss in good faith appropriate modifications to such background check, preserving to the greatest extent possible the intent of the impermissible element(s) of such background check.

- In the event that any Vendor or Worker possesses a government-imposed license or certificate to lawfully perform their specific role (e.g., agents, brokers, attorneys, banks, third party administrators), such Vendor or Worker is exempt from the requirement of an AIG background check.

4.2 Validated Third Party Program

- If the Vendor has an employee screening program of its own, the program can be audited to ascertain whether it meets or exceeds AIG standards and therefore participate in AIG's "Validated Third Party Program" (as further described below, "Validated Third Party Program"). To the extent that a Vendor is approved as part of the Validated Third Party Program, AIG will allow the Vendor's screening program to satisfy AIG's Worker screening requirements (but for clarity, Vendor itself (i.e., the company) will remain subject to Section 4.1). To ascertain if the Vendor's program meets AIG's Vendor Certification Program standards, the Vendor must fill out one application form for each country in which Vendor is seeking approval under the Validated Third Party Program. To the extent that a Vendor is approved to be a part of the Validated Third Party Program, such approval shall be made on a country-by-country basis.

- Vendors that have existing background screening programs that meet the criteria for the Validated Third Party Program may apply for approval through the Validated Third Party Program following the audit process described in the preceding bullet. If the Vendor previously applied for approval and was denied, the Vendor may seek to correct any shortcomings and reapply for approval.

- Determination of whether, and to the extent, a Vendor meets the criteria to be approved as part of the Validated Third Party Program will be made by the AIG Global Security Head of Investigations.

- Participation in the Validated Third Party Program is contingent upon the Vendor agreeing in its contract with AIG that the Vendor will comply with all standards of the Validated Third Party Program and it will submit to continuing periodic audits of its screening program to ensure compliance with the Validated Third Party Program (and to the extent that this policy is included in an agreement between a Vendor and AIG, such Vendor hereby agrees to the foregoing if it participates in the Validated Third Party Program). The periodic audits may be conducted at any time and may consist of (a) having Vendor submit a new Validated Third Party Program application; and/or (b) having certain Workers with Access selected at random be subject to backgrounds checks performed by Screening Provider. The audit will be conducted by Screening Provider in conjunction with members of the AIG Global Security Investigations Team. Any Vendor found to be non-compliant with the Validated Third Party Program will have their "approved" status immediately revoked.

- All correspondence regarding a Vendor's attempt to obtain Validated Third Party Program approvals will occur amongst the AIG business primary point of contact ("POC"), the Vendor's primary POC and the Screening Provider representative conducting the audit. Final determinations regarding any Validated Third Party Program-related matters may also be distributed to the aforementioned individuals by the Screening Provider representative conducting the audit.

- **Note**: If the Vendor's screening program does not meet the requirements for approval as part of the Validated Third Party Program, the Vendor will be required to participate in the standard AIG Vendor Certification Program. AIG may consider, on a case-by-case basis and

in its sole discretion, whether to permit a Vendor to participate in the Validated Third Party Program while it corrects deficiencies in its screening program in accordance with a written program improvement plan.

4.3 Worker Background Screening Phase

Upon completion of the Worker background check, the Screening Provider's "Security Service Representative" ("SSR") will perform the following:

- Obtain appropriate consent forms from the Worker (e.g., in the United States, as required by the Fair Credit Reporting Act ("FCRA") and applicable state law).

- Compare the results against a pre-approved decision matrix to determine if any adverse information has been developed. All adverse information that falls within the matrix will be flagged and brought to the attention of AIG Global Security, which will adjudicate the background investigation as either pass or fail.

- Upon determination of the background being "Pass" or "Fail," the Screening Provider will notify both the appropriate AIG POC and Vendor POC of the background investigation results. These results will be limited to access approved or access denied; the Screening Provider will not disclose the basis for the decision. Adverse notifications will be distributed in accordance with applicable law (e.g., in the United States, in accordance with the FCRA). Only the Screening Provider and limited AIG Global Security personnel will have access to the background results forms and the data contained therein.

- When adverse information leads to denial of Access, to the extent required by applicable law (e.g., in the United States, the FCRA), the proposed Worker will receive a notification of such denial. The proposed Worker will have five (5) days to respond should he/she believe that the information received during the background check is not factual or accurate. Should the Worker fail to respond during such period or if he/she fails to establish that the background check results were not accurate, to the extent required by applicable law (e.g., in the United States, the FCRA), a second adverse notification letter will be sent to the proposed Worker confirming that they are in fact ineligible to render services to AIG. In addition to the Worker receiving the adverse notification, a Vendor representative will also receive email notification informing them that their Worker will not be allowed Access. Additionally, as detailed in a preceding bullet, similar notification will also be distributed to the AIG POC.

- If negative information is found on the Vendor (i.e., the company) itself, and the information is sufficient enough to fail the risk matrix comparison, the AIG Global Security Head of Investigations and the Screening Provider SSR will coordinate with the AIG contract owner to discuss the results and the best course of action to take at that time.

- Regardless of the eventual screening results of the Vendor and Workers, all pertinent data findings will be maintained in the AIG Vendor Certification Program database.

5. Revocation

- Access to AIG facilities, systems and information is a privilege. Without limiting anything set forth in the remainder of any agreement between AIG and a Vendor, permission for such access may be revoked by AIG Global Security, including in connection with unsanctioned, negligent, or willful action on the part of a Vendor, or its Worker(s). This may include, but is not limited to, exploitation of sensitive systems and/or data, introduction of malicious and/or unauthorized software, unauthorized modification or disclosure of systems and/or data, or failure to follow prescribed access control policies and procedures.