GLOBAL VENDOR CERTIFICATION PROGRAM

SUMMARY FOR VENDORS

Global Investigations Division, AIG Global Security

AIG GLOBAL VENDOR CERTIFICATION PROGRAM – SUMMARY FOR VENDORS

1. Purpose

American International Group, Inc. and its subsidiaries (collectively, "AIG" or "we" or "our") have developed mutually beneficial relationships with our vendors and associated standards and policies to ensure such vendors are highly qualified and reputable. This document ("Vendor Summary") is a summary for vendors of our screening program ("AIG Vendor Certification Program") that was established to ensure that those standards are met and adhered to by all (a) AIG vendors and their subcontractor(s) (each, a "Vendor"); and (b) Vendor employees and contractors providing services to AIG (collectively, "Workers") who require Access (as defined below). In the event that this Vendor Summary is included in an agreement between AIG and a Vendor, all capitalized terms defined in this Vendor Summary shall be applicable only to this Vendor Summary.

2. Scope

The terms of this Vendor Summary 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.

Note: Required screening under the AIG Vendor Certification Program of a Vendor and its Workers requiring Access must be complete before such Vendor and such Workers may provide services to AIG.

3. Requirements

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

a. **Vendor Screening**. Vendor screening is conducted as part of the AIG's third party risk management processes. Vendor screening is required during onboarding and every 5 years thereafter. Privately held companies and their owners with 5% or greater interest are required to undergo Vendor screening.

   - *Exemptions*. Publicly traded companies are exempt from Vendor screening due to being subjected to a stringent governmental review prior to their stock exchange listing.

b. **Worker Screening**. Worker background checks are required for any Worker requiring any of the following ("Access"): (a) routine unescorted access to AIG facilities (owned or leased) and / or (b) any access to AIG systems or networks.

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

   - In the event that any Worker 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.

- *Exemptions*.
  - Validated Third Party Program. Worker screening by the Screening Provider is not required if Vendor's own screening program is approved as part of the "Validated Third Party Program" described in Section 4.2 below.
  - Government-imposed License. In the event that any Worker (or their employer) possesses a government-imposed license or certificate to lawfully perform their specific role (e.g., agent, broker, attorney, law firm, physician, physician assistant, registered nurse, hospital, accountant, accountancy firm, bank, third party administrator, independent commissioner-director, state/federal auditor, or similar government regulated role), such Worker is exempt from the requirement of a background check by the Screening Provider.
  - Property Owner Personnel. In certain cases, certain resources engaged by a property owner such as cleaning personnel, security, engineers, property management staff will be exempted from background screening by the Screening Provider.

4. Worker Background Check Process

4.1 Website for Worker Applications

- Workers that require Access must visit the website designated by AIG (currently www.aigscreen.com/kiosk) to prepare and submit their applications and all appropriate consent forms.

4.2 Participating in the 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. To ascertain if the Vendor's screening 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.

- 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's screening program 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 a recertification of its screening program every (5) years to ensure compliance with the Validated Third Party Program (and to the extent that this Vendor Summary 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 recertification consists of having Vendor submit a new Validated Third Party Program application for review by AIG Screening Provider in conjunction with members of the Global Investigations Division (GID) of AIG Global Security. Any Vendor found to be non-compliant will have 90 days to rectify deficiencies and undergo another review. During this time, validated status will remain in place as "under review". If the Vendor does not rectify deficiencies in this period, such Vendor will be removed from the validation program and new Vendor Workers with AIG access as described in Section 3 would be required to undergo an AIG Screening Provider background check.

- 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, GID and the Screening Provider representative conducting the recertification review. 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 review or by members of GID.

4.3 Worker Background Screening

From start to completion of the background check, the Screening Provider will be responsible for the following, some of which in conjunction with GID:

- Obtain appropriate consent forms (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 GID, 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 GID personnel will have access to the background results forms and the data contained therein.

- When adverse information leads to denial of Worker 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.

- 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 or networks 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 GID, 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.