Third Party Screening Requirements, Exceptions, Process and FAQs

I. Company Requirements

Company Background Check Due Diligence requires screening of:

- Third Party Privately Held Companies and
- Principal Owners with 5% or greater interest regardless of interaction or knowledge

  Note:
  - Companies exclusively owned by another company; NO principal background required
  - If ownership includes a company & individuals, or entirely individuals, only individuals with 5% or more interest require screening

II. Exceptions

- The company has government imposed licensing/certification requirements

  Note: *The licensing/certification must be a government mandated standard. Issuance is only granted through comprehensive government reviews or testing, combined with being a government regulated requirement to lawfully conduct associated business, (e.g. agents, brokers, attorneys/law firms, physicians/hospitals, certified public accountants, banks, insurance companies, third party administrators, independent commissioners/directors, state/federal auditors, etc.)*

  **********Business licensing obtained / purchased through a city, state or jurisdiction does NOT qualify for this exemption. This type of licensing is generally issued to provide government with data on the types of business taking place in their jurisdiction so that applicable taxes/fees can be imposed.*

- The company is publicly traded or owned by a public company, (personnel require screenings)
- The background check or specific elements violates local laws, regulations, or customs

III. Process

STEP 1: AIG contract owner or relationship manager sends request to screening vendor Cisive to initiate a private company screening.

- Email Doreen Borgo (dborgo@cisive.com) with the vendor company name, address, company contact name, email, and phone. (CC Jim Meyerdierks jmeyerdierks@cisive.com and Danny Johnston djohnston@aig.com).
- Cisive will email the company contact a client ID and temporary password to complete the company application within the AIG/Cisive screening kiosk/portal.
- Prior to the company contact logging into the kiosk, the AIG contract owner or relationship manager must provide them with the following info as it will be needed during the registration process:
  - AIG manager's name, email address, and telephone number.
  - Business Unit CBD Code or Cost Center.

STEP 2: Principal Owners will register for their backgrounds within the AIG/Cisive screening kiosk/portal at: http://www.aigscreen.com/kiosk/.

- Use the self-invite selection located near the bottom of the web portal page: "*If you have NOT received a username and password for AIG Kiosk Screening, please click here*".
- The registration page will open where they will select "*a principal of a company*" in the "*I am*" section and complete the personal data segments. Registering will require the AIG contract owner or manager information as is listed in Step 1, bullet 3.
- Once registered, the contract owner or manager will receive an email requesting approval of the CBD Code or Cost Center entered by the principal owner during their registration.
- When approval is acknowledged, the principal owner will receive an email containing an individual log-in and temporary password. They must then return to the web portal kiosk and complete the screening application along with e-signing all necessary forms.

STEP 3: Upon Contract Execution, third party personnel (employees, contractors, and subcontractors) requiring access to AIG facilities, systems or data must register to complete individual background checks as listed in STEP 2. For individual Background Checks, however, when the registration page opens, the individual selects "*an employee of a company*" in the "*I am*" section.

IV. FAQs

Exception Related Questions:

Q: I'm a contract owner for a company that is a subsidiary of a publicly traded company; are they required to go through the background check process?
A: No. Subsidiaries of publicly traded companies are exempt the same as the parent company. However, their personnel (employees, contractors and subcontractors) requiring access to AIG facilities, systems or data must be screened.

Q: I have a third party from a country where criminal background checks are heavily regulated and are only allowed to be conducted by government personnel or risk penalties and imprisonment. Is this company still required to be background checked?
A: No, as the background check or specific elements of it would violate local laws, regulations, or customs and would put AIG at risk of a business interruption and/or substantial monetary penalties.

Q: I manage a cleaning service vendor that does not want to go through the background check process as they will only have access to an AIG building, not systems or data. Should I tell them its not required or will I need to submit an AIG Operational Risk Acceptance request?
A: This requires a two-part answer.
First:
Third parties requiring access to AIG facilities, systems or data must be screened unless they meet any of the exception standards listed on page one.
Secondly:
Extreme circumstances must exist before an Operational Risk Acceptance can be submitted as senior leadership prefer not to put AIG at risk by circumventing established controls. A risk acceptance requires business unit management to present comprehensive explanations that justify the risk and business need.

CBRA Related Questions:

Q: The CBRA shows that a company background check is required; does it automatically initiate the background screening?
A: No. The company screening must be initiated by a representative of the third party company as noted in Steps 1-2 on the previous page.

Q: Is the IT Security EAS, SSA or VCAQ reviews the same as a background check?
A: No. These reviews are based on IT Security related items.

Q: Can Global Security answer all questions related to the CBRA?
A: No, only questions related to the background check process.

General Questions:

Q: I am onboarding a consultant and want to get these processes completed as quickly as possible. Can I go ahead and request their EID, email address and systems access before or during their background check?
A: No. AIG policy mandates that third party personnel must have a cleared background check prior to obtaining access to AIG facilities, systems or data.

Q: The third party I manage states they have been validated by Global Security to conduct their own backgrounds and that all their personnel have already been screened when hired by that company, so no background check from the AIG vendor is required. Is that true?
A: Yes, vendors participating in Global Security's "Validated Third Party Program" have had their in-house screening program audited by AIG where it was determined their screening elements met AIG standards and received approval to conduct their own backgrounds of personnel engaged with AIG. A list of validated companies is available for review at the following link: Validated Third Party Program List

Q: I have a third party that has voiced concerns about entering personal information into the screening vendor's background check kiosk. Is their information safe and who will have access to it.
A: Background check information is confidential and only shared with authorized AIG staff on a strict "need to know" basis that is consistent with applicable law. All background data is encrypted and maintained within the screening vendor's US Data Center systems. The screening vendor has never experienced a data breach due to the application of various mechanisms, firewalls, and technological tools at their data housing sites. Background check information is never sold, transferred, or exposed to outside parties.

Q: What happens if negative information is discovered in a third party's background check?
A: This requires a two-part answer as the response would be different for the third party company and personnel.
Company:
If adverse information is discovered, and the information appears sufficient enough to disqualify the vendor, Global Security will coordinate discussions with the contract owner on likely next steps. This discussion may require AIG business unit leadership, Compliance, Legal, or other stakeholders. Depending on the severity of the adverse information, if the decision is made to move forward, it may require the contract owner to submit an AIG Operational Risk Acceptance.
Personnel:
Adverse background checks are adjudicated based on a pre-determined Decision Matrix containing a list of 82 items, largely comprised of criminal offenses. The adverse data is compared with the items in the matrix where matching elements require a disqualification. Any adverse data not listed in the matrix requires a review of its context to ensure it would not pose a risk to AIG or personnel. Adverse data having limited risk would be cleared. All disqualifications follow Pre-Adverse notification criteria allowing the worker a five day response timeframe to dispute the adverse findings. Failure to respond or provide proof the adverse results were not accurate generates an Adverse notification of ineligibility.

Contacts
For further information or queries please email the AIG Global Security, Global Investigations Division at GID@aig.com