Third Party Screening Requirements, Exceptions, Process and FAQs

I. Requirements

The following criteria provide guidance determining when Global Security's screening vendor should be engaged for background checks. It applies to all third parties requiring any of the following accesses:

- Routine unescorted access to AIG facilities (owned or leased), **and/or**
- Access to AIG systems, networks, or applications, **and/or**
- Access to AIG Company Information (excluding Publicly Accessible), regardless of the time period or location, to include any form of remote access or manner in which AIG information / data is received.

NOTE: the term "AIG Company Information" includes Firm Confidential, Customer/Employee Confidential, and Restricted. For further clarification please refer to the AIG Global Information Handling Policy and Standards.

II. Exceptions

1. The company/personnel are covered by a type of government imposed licensing/certification to lawfully perform their specific role (e.g. agents, brokers, attorneys, banks, certain TPAs, etc.)
2. The third party company is publicly traded, however personnel with access to AIG facilities, systems, or data require screenings
3. The background check or specific elements of it would violate local laws, regulations, or customs
4. The third party company / personnel does not require access to AIG facilities, systems, or data
5. AIG Operational Risk Acceptance. Considered a last resort. Not favored by senior leadership.

III. Process

STEP 1: Define the third party company ownership. It will determine the extent of the screening process:

- **Privately Held Companies**: Two-part screening process:
  - Third Party Company
  - Third Party Personnel (employees, contractors, and subcontractors) with access to AIG facilities, systems, or data. **NOTE:** for CBRA purposes, this step, outlined in Step 4 below, can be postponed until access is required.
- **Publicly Traded Companies**:
  - No company screening required due to stringent governmental review prior to stock exchange listing.
  - Conversely, the third party's personnel (employees, contractors, and subcontractors) with access to AIG facilities, systems, or data are still required to be screened.

NOTE: Third party backgrounds are valid for 5 years. If you're not sure if the company has been previously screened by Cisive, contact Danny Johnston (djohnston@aig.com).

STEP 2: AIG contract owner or manager sends a request to the screening vendor Cisive to either initiate a private company screening or request that Cisive enter the exempt public third party in their database.

- Email Doreen Borgo (dborgo@cisive.com), cc'ing Jim Meyerdierks jmeyerdierks@cisive.com) and Danny Johnston (djohnston@aig.com).
- Provide the vendor company name, company contact name, email, and phone.

STEP 3: Cisive will respond to the private company contact with a client ID and temporary password to complete the company application within the AIG/Cisive screening kiosk.

- Prior to the private company contact logging into the kiosk, they need to obtain the following info from the contract owner or manager as it will be needed during the application process:
  - AIG manager's name, email address, and telephone number.
  - Business Unit CBD Code or Cost Center.

STEP 4: Third Party Personnel (Employees, Contractors, and Subcontractors) with access to AIG facilities, systems, or data will register for their backgrounds within the secure AIG/Cisive web portal kiosk 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".
- Choose "an employee of a company" in the "I am" section of registration and complete the personal data sections. Registering will require entry of the contract owner or manager info listed in Step 3.
- Once registered, the contract owner or manager will receive an email requesting approval of the CBD Code or Cost Center entered by third party personnel during their registration.
- When approval is acknowledged, third party personnel 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.

IV. FAQs

Exception Related Questions:

Q: I have a vendor that has a city license in order for them to conduct business in that city. Does this apply to the exception standard?

A: No. Licenses, certifications, or permits acquired by companies/personnel to work in a specific location (cities, states, regions or countries) and/or to receive permission to conduct a specific kind of business or trade in those locations, do not qualify. These types of government imposed requirements are only mandated for tax purposes and/or to make local government aware of who or what is working in the areas they govern.

NOTE: The licensing / certification exception applies to companies/personnel that have qualified through government imposed regulations requiring stringent standards do be met in order to conduct a particular type of business, or through an educational process requiring an individual to qualify for a particular business role by meeting rigorous testing standards to obtain and maintain their license or certification.

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 third party relationship with a company that will have access to AIG public company information but have no need to access AIG systems or facilities. Will this company require a background check?

A: No. Public information is available to everyone. The term AIG Company Information specifically relates to Firm Confidential, Customer/Employee Confidential and Restricted.

Q: The vendor I manage does not want to go through the background check process as they will only have access to an AIG building, not systems or data as they are only a cleaning service. 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 1-3 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. The background check covers the following: 1) US Federal Criminal and Civil or if outside the US, the International equivalent, 2) US County & State Criminal and Civil or International equivalent, and 3) Liens and Judgements.

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 am getting ready to onboard a privately owned third party company and remember that the company and its principal owners holding 5% or greater interest in the company must be screened. Is that still mandatory?

A: No. Only the company screening is required. Principal owner screenings have been discontinued.

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.