# DESIGNATE AN INSIDER THREAT SENIOR OFFICIAL

**Requirements:**

The NISPOM has identified the following requirements for the designation of an Insider Threat Senior Official under paragraphs 1-202b and 2-104:

- **U.S. Citizen**
- **Employee**
- **Cleared in Connection with the Facility Clearance**
- **The Insider Threat Senior Official must always be cleared to the level of the facility clearance (FCL)**

**Getting Started:**

The Insider Threat Senior Official may be the FSO or any other employee that meets the requirements. If the FSO is not chosen as the Insider Threat Senior Official, the FSO must still be an integral member of the facility's Insider Threat Program. A corporate family may choose to implement a corporate-wide Insider Threat Program with one senior official designated to establish and execute the program. Each cleared legal entity using the corporate-wide Insider Threat Program Senior Official must separately designate that person as the Insider Threat Senior Official for that legal entity and include them on the Key Management Personnel (KMP) list. When a division or branch has been granted an FCL based on requirement for safeguarding, the division or branch may designate the corporate-wide Insider Threat Program Senior Official as a KMP or designate a different employee to be the Insider Threat Program Senior Official at the division or branch.

The selected official must receive training on key topics related to Insider Threat and be able to demonstrate the effectiveness of their Insider Threat program to the CSA. The senior official will be responsible for implementation of the plans, processes, procedures and response protocols under the Insider Threat Program at the facility.

**Best Practices:**

- In line with the training topics designated for Insider Threat Program personnel, it is a good idea to keep up to date on topics related to counterintelligence, security and defensive security fundamentals; laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data (including the consequences of misuse of such information); and applicable legal, civil liberties, and privacy policies. Awareness of legal and policy changes, both internal to your company and at the state, local, and federal level, will ensure that all elements of the program run smoothly.
- When establishing procedures for conducting Insider Threat response actions, look to existing company policy and industry standards.

**Related Training and Resources:**

- **eLearning Course: Establishing an Insider Threat Program for Your Organization CI122.16**
- **Insider Threat Toolkit Tab: Establishing a Program**