INSIDER THREAT AWARENESS

In light of the increased risk of terrorism and severe criminal activities, like workplace violence and cybercrime, SCIS is training its employees about insider threat awareness with a theme of, "See Something, Say Something"™. This is an essential component of a comprehensive security program. SCIS encourages employees to report suspicious activities observed while on duty.

SCIS has customers in many different industries. Some of these businesses could be targets for terrorist attacks or other kinds of serious crime. High importance sites such as airports, classified facilities, petrochemical and power plants are obvious potential targets, but any site may be a target.

In providing a security program, SCIS employees have access to customer sites. The *insider threat* derives from the risk that **someone would use his/her employment position to carry out, facilitate or enable terrorist or other criminal activities**.

An employee might act on his/ her own initiative or be a target for insider recruitment. Criminals who recruit insiders are smart and target persons who have valuable information or are vulnerable in some way. Employees that may be recruited include:

- Employees with a Personal Security Clearance (PSC)
- Employees working at strategic sites (airports, classified facilities, petrochemical and power plants, etc.).
- Employees with excessive debt, gambling debts, etc.
- Employees who have suffered a life crisis (death of a friend or family member, divorce, depression, etc.).
- Employees who complain repeatedly that they have been treated unfairly either by the government or their employer.
- Employees who do not seem to fit into mainstream society.
- Employees who become zealous proponents of radical ideas.

So what can we do to mitigate insider threat risk? First, it is important to be aware of the risk and signs that could reveal an insider threat. Signs to look for:

- Changed behavior –towards colleagues and in social media, extensive spending of money, changed behavior towards the opposite sex, changed clothing or eating habits, etc.
- Questioning – An employee asks questions about the facility or about sensitive information that falls outside his/her area of responsibility.
- Photos – An employee takes photos or in some other way documents the customer site.
- Tests of Security - attempts to penetrate or test the physical security or the security procedures at the targeted site. An employee may attempt to enter the site without proper access control authorization in order to test the security response.
- Remember, insider threat risk is not based on race, ethnicity or religion – it is the behavior that is the focus.

Stay informed about the terrorism exposure in your state, city, and/or client site and follow internal policies and procedures. Immediately report any suspicions you may have of someone that could be using his/her employment to carry out, facilitate, or enable terrorist or other severe criminal activities.

There are several different ways to report your suspicions:

- The SCIS Hotline – 1-800-574-8637, www.scishotline.com
- To your Human Resources representative
- To your manager

It is important that you are aware of the risks and the signs, but it is equally important that we discuss the insider threat risk without prejudice. SCIS is an Equal Opportunity Employer and has a policy of treating all employees with respect and dignity. Insider Threat reporting should not be used to report false claims against a co-worker as SCIS takes all reports seriously and will investigate, and where appropriate, report to the local authorities.

Let's stay vigilant, be aware, and focus on potential harm and strive to work together to ensure our workplace and communities stay safe.