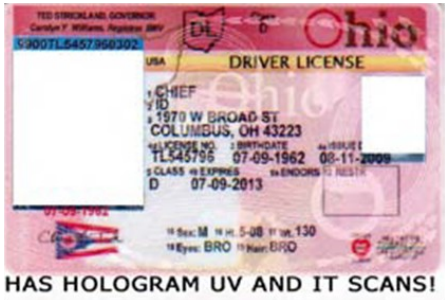
Reportable Indicators or Activities

* **Elicitation** – questions beyond mere curiosity
* **Testing of Security** – challenges that reveal physical, personnel or cyber capabilities.
* **Recruiting** – building teams, contacts or personnel data
* **Photography** – perimeters, security cameras, remote access points
* **Observation/Surveillance** - unusual interest in facilities i.e. use of binoculars, note taking, measurements
* **Breach/Attempted Intrusion** - entering a restricted area or site, impersonation
* **Misrepresentation** – false insignia, documents or identification
* **Theft/Loss/Diversion** – stealing badges, uniforms, technology, documents



BOTTOM LINE:

BE ASSERTIVE

BE ALERT

BE AWARE

Reportable Indicators or Activities

* **Cyberattacks** - compromising or disrupting the IT infrastructure
* **Expressed or Implied Threats** - spoken or written threats to damage or compromise facilities
* **Material Acquisition/Storage** - unusual quantities of cell phones, pages, fuel
* **Acquisition of Expertise** – obtaining or conducting training in security, weapons or tactics
* **Weapons Discovery** - unusual amounts of weapons, ammunition or explosives
* **Sabotage/Tampering** - damaging, defacing or manipulating property

Report IAW AR381-12

Your Army Counterintelligence Covering Agent Is:

Office - 655-1306
Duty Agent Phone - 954-5567

Reporting THE THREAT

This product created by a MICECP
1640 Lyman Road Bldg x3050,
Schofield Barracks, HI. 96857
808-655-1126

ARMY Counterintelligence

Army Counterintelligence works to protect Department of Army personnel, technology and classified information that resides in each unit and to enhance CI/CE/LE partnerships and information sharing among public and private organizations.

Prompt reporting of foreign collection attempts is critical to an effective CI program. Immediately notify the nearest CI office should you have any reason to believe that your unit or one of its members has been a target of a foreign collection attempt.

Terrorists generally do not provide a preemptive warning and they methodically conduct surveillance/ reconnaissance of an objective prior to an attack. DoD personnel can mitigate the risk by using some of the following tips:

- Awareness is a powerful weapon
- Knowledge of terrorist techniques & methods can help prevent an attack
- Random antiterrorism measures (RAM) make life difficult for prospective terrorist
- Static defenses increase friendly risk; make constant adjustments to avoid this scenario
- Be creative, "highly visible and unpredictable"
- Assessments sustain active improvements in defensive posture
- Include terrorist considerations into your Intelligence preparation
- Maintain solid link with nearby CI office

THREAT

These indicators by themselves do not positively guarantee an individual may have ties to terrorism; however, they serve as a guide to the listed indicators and patterns.

- Young (17-35 years)
- Loitering (Repeat appearances in the same area)
- Nervous
- Measuring distances
- Avoiding Law Enforcement
- No readily apparent reason for being at the site
- Asking security related questions
- Taking notes
- Cell phone picture taking
- Video/Pictures of unusual places
    - Gates
    - Entry ramps
    - Bridges
    - Personnel manning access points
    - Barriers
- Driving rental car

METHODS