2016 Joint Annual NDIA/AIA Industrial Security
Defense Security Service Panel

May 17, 2016
Problem Statement

Compliance is **not** a purpose unto itself

In today’s threat environment, unprecedented in our history, **our efforts** must be effective, and ideally efficient, which means risk-based, focused on rooting out threats and vulnerabilities to minimize/eliminate adversarial impact to classified programs.
Methods of Operation

**Academic Solicitation**
Via requests for, or arrangement of, peer or scientific board reviews of academic papers or presentations, or requests to study or consult with faculty members, or applications for admission into academic institutions, departments, majors, or programs, as faculty members, students, fellows, or employees.

**Suspicious Network Activity**
Via cyber intrusion, viruses, malware, backdoor attacks, acquisition of usernames and passwords, and similar targeting, these are attempts to carry out intrusions into cleared contractor networks and exfiltrate protected information.

**Attempted Acquisition of Technology**
Via agency of front companies or third countries or direct purchase of firms, these are attempts to acquire protected information in the form of controlled technologies, whether the equipment itself or diagrams, schematics, plans, spec sheets, or the like.

**Seeking Employment**
Via résumé submissions, applications, and references, these are attempts to introduce persons who, wittingly or unwittingly, would thereby gain access to protected information that could prove useful to agencies of a foreign government.

**Request for Information**
Via phone, email, or webinar approaches, these are attempts to collect protected information under the guise of price quotes, marketing surveys, or other direct and indirect efforts.

**Solicitation or Marketing Services**
Via sales, representation, or agency offers, or response to tenders for technical or business services, these are attempts by foreign entities to establish a connection with a cleared contractor vulnerable to the extraction of protected information.

**Foreign Visit**
Via visits to cleared contractor facilities that are either pre-arranged by foreign contingents or unannounced, these are attempts to gain access to and collect protected information that goes beyond that permitted and intended for sharing.

**Exploitation of Relationships**
Via established connections such as joint ventures, official agreements, foreign military sales, business arrangements, or cultural commonality, these are attempts to play upon existing legitimate or ostensibly innocuous relationships to gain unauthorized access.

**Surveillance**
Via visual, aural, electronic, photographic, or other means, this comprises systematic observation of equipment, facilities, sites, or personnel.

**Criminal Activities**
Via theft, these are attempts to acquire protected information with no pretense or plausibility of legitimate acquisition.

**Search/Seizure**
Via physical searches of persons, environs, or property or otherwise tampering therewith, this involves temporarily taking from or permanently dispossessing someone of property or restricting his/her freedom of movement.