

EXPLANATION OF INSA-DEVELOPED INSIDER THREAT DEFINITION

In November 2015, the INSA Insider Threat Subcommittee, under the auspices of the Security Policy Reform Council (SPRC), undertook an initiative to refine the definition of Insider Threat. The Subcommittee of representatives from the U.S. Government and Industry noted three issues:

1. Many government and industry definitions already exist.
2. A majority of them are not inclusive, failing to account for one or more aspects of threats posed by an insider.
3. Several industries are struggling with the threats posed by insiders, and many articulated that existing definitions created barriers to efficient implementation of insider threat programs.

Through group discussion, several proposals were made, subjected to critical peer review. The Subcommittee settled on the below language, briefed to and embraced by SPRC on December 4, 2015. The Directors of the Defense Security Service and the National Counterintelligence and Security Center were also briefed, both of whom endorsed the inclusive nature of the definition and the language specific to instances of workplace violence.

Insider Threat:

The threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly, or unwittingly, commits: acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace.

An explanation of the definition:

- The concise, yet inclusive nature is designed to relate to all U.S. industries and Government. Several definitions we reviewed are easily interpreted to focus only on the U.S. Government or the Defense Industrial Base, to the exclusion of other industries such as, but not limited to, Energy, Finance, Oil and Gas, and Pharmaceutical.
- Insider threat explicitly refers to a human being.
- "Authorized access" refers to a person who has successfully gone through agency or company vetting processes, prior to a final hiring decision, granting them access to facilities, other employees, information, networks, and other resources.
- "Wittingly or unwittingly" recognizes that the threat could have been posed by a person purposefully, accidentally, or neglectfully.
- "Acts in contravention of law or policy" requires that either a law or stated policy or practice was violated.
- The harm in "Harm through the loss or degradation..." is determined by company or agency.
- Inclusion of language regarding "workplace violence" had everything to do with how "insider" was defined—a person granted access to people and facilities based on some form of vetting that resulted in a hiring decision.