#### Business Use Cases

1. Large Company Use Case – This use case is concerned about the ability of large corporations to effectively articulate a threat and risk landscape, covering threats from a wide area of security threats, including: information and communication systems (cyber), facilities, personnel, geopolitical, pandemic/medical threats, etc.
2. Critical Infrastructure - Power, water and other critical infrastructure are threatened by cyber and physical terrorism. Industrial Control Systems are increasingly computer controlled and connected (directly or indirectly) to the internet and may embed compromised control hardware/software from questionable sources. Critical infrastructure is subject to combined physical and Cyber threats.
3. This ISE-SAR Functional Standard is designed to support the sharing, throughout the Information Sharing Environment (ISE), of information about suspicious activity, incidents, or behavior (hereafter collectively referred to as suspicious activity or activities) that have a potential terrorism nexus. The ISE includes State and major urban area fusion centers and their law enforcement, homeland security, or other information sharing partners at the Federal, State, local, and tribal levels to the full extent permitted by law. In addition to providing specific indications about possible terrorism-related crimes, ISE-SARs can be used to look for patterns and trends by analyzing information at a broader level than would typically be recognized within a single jurisdiction, State, or territory. Standardized and consistent sharing of suspicious activity information regarding criminal activity among State and major urban area fusion centers and Federal agencies is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities associated with terrorism. This ISE-SAR Functional Standard has been designed to incorporate key elements that describe potential criminal activity associated with terrorism and may be used by other communities to address other types of criminal activities where appropriate. Suspicious activity is defined as observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. A determination that such suspicious activity constitutes an ISE-SAR is made as part of a two-part process by trained analysts using explicit criteria. Some examples of the criteria for identifying those SARs, with defined relationships to criminal activity that also have a potential terrorism nexus, are listed below
   1. Expressed or implied threat
   2. Theft/loss/diversion
   3. Site breach or physical intrusion
   4. Cyber attacks
   5. Probing of security response

#### Technical Use Cases

1. Pivoting through SITX and NIEM to exchange new threat information, e.g. between CSIRTs.
2. Assessing threat and risk of a given cyber system; this involves using the elements of the conceptual model to structure the report and sharing the report, e.g. with the stakeholders and partners
3. Aligning risk models along the dependencies between systems;
4. Exchange of global information supporting assurance of risk assessment, including taxonomies of assets, threats, injury types, threat activity types, capabilities, motivations, etc.