OT/ICS Sector Engagement Working Group: Kick-Off Call Executive Summary

Executive Summary:
The OT/ICS Sector Engagement Working Group is tasked with understanding the **stakeholders, dependencies, barriers, leverage points, and opportunities surrounding life-safety-critical functions**, with particular attention to organizations that lack the resources, information, or incentives available to operators with more resources. The discussion repeatedly stressed two distinctions: the project is focused on **functions rather than entire critical-infrastructure sectors**, and on the operational realities of the "have-nots" rather than the well-resourced organizations with which cybersecurity experts frequently interact.

A central objective is to identify the organizations and relationships upon which critical functions actually depend. The group discussed examining **first-, second-, and third-order effects**, essentially treating disruptions as having a "blast radius." Rather than exhaustively mapping every organization, the working group should identify representative dependencies and develop a repeatable methodology that others can subsequently extend.

One of the strongest themes was the importance of **system integrators, vendors, and other intermediaries as leverage points**. Smaller operators frequently rely heavily on integrators to design, install, maintain, and configure operational systems. Consequently, improving practices among a comparatively small number of integrators or vendors could potentially improve resilience across a much larger number of operators. This approach may be more realistic than expecting thousands of small organizations to independently acquire sophisticated cybersecurity expertise.

Participants also argued that cybersecurity should increasingly resemble **safety engineering**: protections should ideally be built into systems and processes rather than requiring constant intervention by individual users. The group drew parallels to the evolution of workplace safety, where practices that were once treated as specialized responsibilities became embedded into normal operations and design.

Terminology and communications emerged as another important consideration. Several participants cautioned against labels when discussing operators who are resource constrained. The project's internal terminology may therefore evolve. The group also needs to use language familiar to operators—describing recognizable operational failure modes rather than imposing cybersecurity terminology on audiences that may not identify themselves as cybersecurity stakeholders.

Given the breadth of the problem, the group leaned toward going **"deep and narrow" rather than "broad and shallow."** A smaller number of life-safety-critical functions can be examined in depth if the resulting methodology is sufficiently clear for others to replicate. Subgroups or "tiger teams" may separately investigate consequences, dependencies, leverage points, friction, and opportunities or particular functions.

Immediate next steps: The group will determine how to divide work among smaller teams and begin applying its framework to selected life-safety-critical functions. The emphasis will be on producing concrete examples while documenting a methodology that can be replicated across additional functions after the 100-day sprint.