Novel Mitigation Analysis Working Group: Kick-Off Call Executive Summary

Executive Summary:
The Novel Mitigation Analysis Working Group began with an intentionally broad mandate: identify **unconventional or underused approaches that could materially reduce the likelihood or consequences of cyber incidents affecting life-safety-critical functions**, particularly where conventional cybersecurity practices are inadequate or unrealistic. The initial phase is deliberately focused on generating ideas rather than prematurely constraining the solution space.

The co-chairs set a relatively modest definition of success: identifying even **two or three genuinely useful novel mitigations** that survive rigorous evaluation would represent a meaningful outcome. Proposed ideas will ultimately need to be tested against the realities facing actual owners and operators, especially resource-constrained organizations. The group therefore plans to engage operators to determine whether proposed mitigations are technically, legally, economically, and operationally feasible.

Initial discussion demonstrated the breadth of approaches under consideration. Participants raised ideas involving **large-scale exposure identification and adversarial emulation, changes to legal authorities or acceptable-use arrangements, automated or distributed mechanisms for reducing the functionality of insecure devices, and approaches drawn from scientific and engineering disciplines rather than traditional cybersecurity controls**. The discussion also touched on more controversial concepts in which third parties might intervene when operators fail to mitigate serious risks.

A key analytical question emerged around **why operators fail to act**. Rather than assuming inaction is irrational or negligent, the group wants to understand why an operator's cost-benefit calculation may differ from that of policymakers or security experts. That distinction could determine whether the appropriate mitigation is technical, economic, legal, regulatory, or organizational.

The group also emphasized drawing inspiration from **other disciplines**. Novelty does not necessarily mean inventing an entirely new technology; it may mean importing an established concept from another field and applying it to cybersecurity or critical infrastructure in a new way. Ideas will eventually be assessed for effectiveness as well as risks, unintended consequences, implementation barriers, and operator acceptance.

Because the brainstorming process may involve controversial or preliminary ideas, participants were instructed to treat discussions as **confidential unless the contributor explicitly authorizes wider sharing**. This is intended to allow the group to explore ideas freely before determining which should become formal recommendations.

Immediate next steps: The co-chairs will organize the initial ideas into a shared workspace and establish an evaluation structure. Members will continue contributing potential mitigations

asynchronously, with a likely weekly meeting cadence. Promising concepts will subsequently be tested with relevant owners and operators.