ASPEN CYBERSECURITY GROUP

THE ASPEN INSTITUTE

Operational Collaboration Task List

Collaboration Frameworks

1. Convene a multi-stakeholder process to develop criteria for which private sector entities should be involved in operational collaboration activities and to identify an initial list of those entities *(NIST & DHS*)

Intelligence and Information Sharing

1. Create criteria for private sector participation in full-cycle of intelligence relationships *(DHS, sector specific agencies, & sector-coordinating councils)*
2. Establish routinized full cycle intelligence relationships in classified settings with private sector designated operational hubs that meet criteria *(ODNI & DHS)*
3. Develop use cases for threat intelligence sharing and the intelligence needed to support those use cases *(industry)*

Risk Management

1. Conduct research to model potential cross-sector systemic failures due to cyber incidents *(DHS, NIST, Dept. of Energy Labs, FFRDCs, & academic institutions)*
2. Collaborate on research on potential cross-sector systemic failures *(industry)*

Contingency Planning

1. Work with private sector operational organizations to identify scenarios where the combination of capability and threat against national critical function is specific enough for which we need new and/or updated contingency plans. *(DHS, DOD, & industry)*
2. Conduct national level contingency planning workshop to identify national cyber-attack contingencies and approaches for planning, resourcing, and exercising responses as well as necessary training. *(DHS, DOD & industry)*
3. Develop new and/or update joint contingency plans incorporating a whole-of-nation response, and ensure they are shared with all relevant interagency partners and sector stakeholders. *(DHS, DOD, & industry)*
4. Conduct training and exercises with all relevant interagency partners and private sector stakeholders once contingency plans have been established. *(DHS, DOD, & industry)*

Offensive Cyber Operations

1. Establish a firm definition of offensive cyber operations and ban on commissioning or engaging in offensive cyber operations by private entities. *(Congress)*
2. Establish processes for assessing response options and risks in an operational environment that includes private sector input. *(DHS, DOD, & private sector)*
3. Support government-led offensive cyber operations as appropriate. *(Private sector)*

Product and Public Policy

1. Define safe harbor parameters for the private sector regarding regulatory reactions to incidents. (*Regulatory agencies)*
2. Establish consistent definitions for mandatory reporting triggers for incidents. (*Regulatory agencies*)
3. Establish reasonable timeframe to report incidents, which includes time to investigate incident and ensure only actual incidents are reported (i.e. prevent reporting of false alarms). (*Regulatory agencies)*
4. Create legal framework for operational collaboration activities (i.e. anti-trust exemption; liability protection). *(Congress)*