Summary of Encrypted Network Interface Unit Breakout Sessions

1. Adding dynamically determined ephemeral encryption to existing Network Interface Unit components deployed in emerging weapon systems will simply operational security issues.

   Rationale: Current platform interoperability is complicated by disparate security classification guidelines and the growing number of participants and collaborating forces in modern engagements. Even without the need to isolate communication between members of coalition forces, communities of interest are already requiring separation of information flows. However the existing mechanizations that require transactional negotiation of the exchange in content does not support real-time exchange of information. The classic approach of establishing fixed encrypted tunnels to define operational enclaves does not support the dynamics of Net Centric Interoperability.

   Hardware mechanization of the proposed capabilities of the Air Force variant of One Box One Network (OB-1) in support of IPsec, IKEv2 and X.509 functionality would be valuable in supporting the dynamic negotiation required by Communities of Interest in the battle space. Such a modernization could be included in an upgrade to the existing Network Interface Unit component found in a number of emerging weapon systems. By facilitating virtual security tunnels between platforms, mission specific virtual enclaves could be established simplifying the cross platform accreditation process and facilitating interoperability. Though there was some debate about a general requirement for mission dynamic enclave definition relating to weapon systems platforms and their interoperability, there seemed to be consensus that such an technology was worthy of evaluation and may be a reasonable benefit of the current evaluations of the OB-1 efforts.