DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

— **Subcontractor Flowdown to International Suppliers**

- The DFARS is generally written for U.S. contractors, and does not consider complications introduced by foreign partners/sub-contractual relationships
- Potential conflicts have been identified between the requirements of DFARS Clause 252.204-7012 and existing country agreements/national laws in areas such as the reporting of cyber incidents direct to the DoD, the submission of malware and media to the DoD, and providing access to information and equipment.
- OUSD(AT&L) and DoD CIO are currently working with the Department's Defense Technology Security Administration (DTSA), under OUSD(Policy), to resolve these potential conflicts on a country-by country basis, and to provide guidance for U.S. Contractors on how to implement the rule within National Law and Country Agreements.
- An agreement is already in place between the Department's Defense Technology Security Administration (DTSA) and their counterpart in Israel, the Director of Security of the Defense Establishment (DSDE) (attached). We expect that this approach will be somewhat unique in that Israeli companies which fall under the oversight of the DSDE will store all controlled unclassified information on their classified network. As such - there is no "covered contractor information system" and therefore the clause does not apply. For Israeli companies which do not fall under the oversight of the DSDE, DFARS Clause 252.204-7012 will apply as written.
- Efforts to address identify national law and country agreements for the following nations are underway:
  - France
  - Germany
  - Japan
  - Netherlands
  - Norway
  - Spain
  - UK
- Contractors should notify the Department at osd.dibscia@mail.mil if they require assistance with regard to this issue.

The Parties acknowledge that the Office of the Secretary of Defense, Defense Technology Security Administration (DTSA) and the Israeli Directorate of Security of the Defense Establishment abide by the General Security of Information Agreement between the United States of America and the State of Israel of 10 December, 1982 (hereinafter: the Agreement) requiring safeguarding for in country classified systems.

[NAME OF US COMPANY] will transfer unclassified covered defense information to [NAME OF ISRAELI COMPANY] using Secure Cyber Transfer Process.

[NAME OF ISRAELI COMPANY] authorized and trained personnel shall download information using a NIST SP 800-171 compliant stand-alone network, designated solely for the transfer of information. [NAME OF ISRAELI COMPANY] shall transfer information into its classified system.

[NAME OF ISRAELI COMPANY] shall process, store or transmit any unclassified covered defense information on the classified system, safeguarding it in accordance with the Agreement and report cyber incidents that occurred in the unclassified stand-alone system only to [NAME OF US COMPANY]. Cyber incidents involving the unclassified covered defense information that occurred in the classified system will be reported in

accordance with the procedures in the Agreement similar to those for classified incidents.

Under these conditions, per the unclassified covered information system definition, DFARS 252.204-7008 and 252.204-7012 shall not be applicable to [NAME OF ISRAELI COMPANY]