INFORMATION SHARING / CYBER SECURITY BREAKOUT SESSION RECAP

Issue 1:

- **Need methodologies and processes to disseminate threat data throughout the supply chain.**
- **Sub Tier contractors need to be provided information on APT and methodologies to mitigate the threat.**

Action:

- **Allow the prime DSIE members to nominate those sub tier contractors to join the DSIE portal. Additionally develop a process using the GCC/SCC to fund a tiger team to assist the dissemination of threat information to sub tier companies using the National Security Grid model.**

INFORMATION SHARING / CYBER SECURITY BREAKOUT SESSION RECAP

Issue 2:

- **The SCC/GCC need to develop a process for attack correlation to allow a more coordinated response and mitigation**

Action:

- **The GCC should stand up an information sharing cyber sub council to interface with the DSIE. This sub council should then develop a process for event correlation across the DSIE DIB companies to enable preventative steps to halt an attack to other companies and GCC partners. Enable DCISE to participate in the Cyber Security Sub-Council of the GCC?)**

- **Disseminate near real time monitor and sensor alerts to improve situational awareness**

INFORMATION SHARING / CYBER SECURITY BREAKOUT SESSION RECAP

Issue 3:

- **The DoD Service Acquisition are proposing changes to the FAR and DFAR language to require certain security standards for future contracts**

Action:

- **Convene a working group of GCC and SCC members to review the proposed changes and make comments prior to posting to the Federal Register**

INFORMATION SHARING / CYBER SECURITY BREAKOUT SESSION RECAP

Issue 4:

- **Need to develop an information exchange between the DoD and the DIB regarding cyber security issues following the NIPP model of multidirectional and networked. There are currently two programs that involve cyber security; the DCISE as a pilot in the DoD and the DSIE under the DIB SCC.**
- **Need to ensure that sub tier contractors are included on the information sharing and that the program is scalable to include additional cleared and uncleared contractors**

Action:

- **Encourage the DoD Cyber Task force (DCISE) to use the GCC as an interface with the DIB SCC and the DSIE. Structure a trust relationship using a non-disclosure process and the US CERT methodology to share real time cyber intelligence information and continue to enable classified information sharing in an expanded DIBNet architecture.**

INFORMATION SHARING / CYBER SECURITY BREAKOUT SESSION RECAP

Issue 4 “continued”:

Action:

- **Encourage the DoD Cyber Task force (DCISE) to use the GCC as an interface with the DIB SCC and the DSIE. Structure a trust relationship using a non-disclosure process and the US CERT methodology to share real time cyber intelligence information and continue to enable classified information sharing in an expanded DIBNet architecture.**
- **Need to examine DC3 contact and GCC membership. This would give DC3 access to DSIE information through the GCC.**
- **Forum for CIKR and cleared/uncleared contractors together**
- **Use, or integrate the DSIE/NSIE model into DCISE**
- **The DSIE non disclosure agreements (NDA) are a good trust building tool.**

INFORMATION SHARING / CYBER SECURITY BREAKOUT SESSION RECAP

Issue 5:

- **Develop a common taxonomy for incident response between the DoD and the DIB partners**

Action:

- **Use the DSIE/NSIE model**
- **Establish a strategic working group through the GCC/SCC to develop that taxonomy**

INFORMATION SHARING / CYBER SECURITY BREAKOUT SESSION RECAP

Issue 6:

- **A lack of defined process for developing requirements and standards for securing the DoD/DIB cyber space**

Action:

- **<u>Develop a process through the SSP that clearly defines the metric and goals for the cyber security of the GCC/SCC.</u>**

INFORMATION SHARING / CYBER SECURITY BREAKOUT SESSION RECAP

Issue 7:

- **DIB owners/operators need to identify information requirements and provide to GCC. DCISE may consider smaller exchanges to identify and document customer requirements through the GCC.**

Action:

- **SCC conducts survey of owner/operator essential information requirements. The GCC and SCC meet jointly to discuss these requirements as a part of development of the SSP.**

INFORMATION SHARING / CYBER SECURITY BREAKOUT SESSION RECAP

BEST PRACTICES:

- **Information sharing on the attack vectors and methodologies through the DSIE has been very successful. Companies can learn the location of C2 servers and block data exfiltration. This also allows them to quickly identify stealth Trojans on their networks.**
- **DIBNet through the DCISE Cyber task force. The development of the DIBNet should continue as we seek to work within a more real time information sharing structure within the GCC/SCC CIPAC framework. Classified Intel Data needs to be more timely and relevant.**