Question: What if we have a DoD Component that deploys a system or service to another DoD Component but does not provide the necessary reciprocity documents? What's the fix or action?

Answer: The AO receiving component does not have to deploy if she/he does not want to if it is not an Enterprise ATO. DoDI 8500 has a section on reciprocity so if component/agency wants to develop across DOD they follow reciprocity to get an Enterprise ATO granted for the system.

Question: What DoDI mandates the Connection Approval Guide?

Answer: DoDI 8500.01

Question: Will control systems include industrial controls systems (ICS) and FRCS SCADA?

Answer: Yes

Question: Is CJCSI 6211.02 be rescinded?

Answer: If it is going to be rescinded, items need to be moved into 8510. At this time, it is not being rescinded.

Question: Are the working groups internal or external to DISA?

Answer: The working groups are DoD and used to support DoD.

Question: Is there one WG at DISA for the 7 DevSecOps WG?

Answer: No. The June DSAWG will brief the new working groups.

Question: What is the relationship of DSAWG and interconnection of space-based communications and IS systems on earth?

Answer: If a space-based system is used across DoD and there is a vulnerability used then it will come to the DSAWG for risk acceptance.

Question: What is the end result or outcome of the 7 DevSecOps WG task?

Answer: June 8th brief will provide DSAWG with this information.

Question: Is there a technical work group that supports the space-based area?

Answer: There is not a one under the DSAWG.

Question: Has a policy for connection with foreign nation networks been promulgated and if so what is the title?

Answer: Yes. There is a policy letter generated by Joint Staff. The guide is called Partner Nations System Connection Process Guide.

Question: When will new CPG version be posted

Answer: When DoD CIO approves the CPG it will be posted to https://cyber.mil/connect/cpg-website-version/?

Question: Who do we contact to attend the June 7 DSAWG meeting?

Answer: DSAWG contact information is located on https://cyber.mil/connect/help/.

Question: Does the DSAWG also address IAP connections when the IAP affects numerous DoD entities?

Answer: If the Component is looking into implement commercial IAP and changes are made that impose risk then it goes to DSAWG. If the whitelist/blacklist entries are just added the nit does not go to DSAWG.

Question: Does the DSAWG address vulnerabilities introduced by data systems?

Answer: If data systems being accessed across DoD, then it will be addressed at DSAWG level.

Question: When will the DSAWG 101 CBT be updated?

Answer: When the policies are fully approved, we will update the video and post it. No exact ETA.

Question: Is there a link to the DSAWG video?

Answer: https://cyber.mil/connect/mptp

Question: Is there a dial-in or link for DSAWG meetings?

Answer: Contact the DSAWG team to request info. Contact information is located on https://cyber.mil/connect/help

Question: Will there be in person scheduled meetings yet?

Answer: The DSAWG team has not heard anything about conducing the meetings in person. However, when we come back into the office full time, the DSAWG meetings will still probably be conducted using GVS-S for awhile.

Question: Who do we contact for connections and use of ports?

Answer: PPSM Team (https://cyber.mil/connect/help) or TAG rep (https://disa.deps.mil/org/RE4/RE42/PPSM/DoD%20Component%20Contact%20List/DoD%20Component%20Contact%20List_20210513.pdf)

Question: How is PPSM integrated with USAF DevSecOPS 2.0 guideline?

Answer: Contact USAF tag rep.

Question: When it comes to approval of ports is 16000 UDP ports considered too many?

Answer: PPSM has several UDP services that have the ephemeral UDP range listed on the CAL (i.e. SRTP). It depends on the particular use case, boundaries required, etc.

Question: Does the DSAWG get into decisions regarding high risk use of cloud services?

Answer: Yes

Question: Do very low risk CDS skip the CDTAB?

Answer: They do not skip the CDTAB since the CDTAB determines the risk level and makes a recommendation to the DSAWG.

Question: Does that include the SIPRNet telework solution?

Answer: Some SIPRnet mobile devices have been reviewed at the DSAWG.

Question: I'm having problems with opening SRTP ports on a firewall?

Answer: Firewalls manage by application profiles and not by port numbers so there's options to filter and regulate by the AppID.

Question: Where is the link for the CPG 6.0?

Answer: https://dl.cyber.mil/connect/pdf/unclass-DISN_CPG.pdf

Question: How can I find out more information about DevSecOps?

Answer: Send email to DSAWG team. They will get you in touch with appropriate individuals.