BULLET BACKGROUND PAPER

ON

COMPUTER NETWORK DEFENSE-JOINT TASK FORCE (CND-JTF)

PURPOSE

To provide background and current status on the CND-JTF

BACKGROUND

DoD has long recognized that DoD needed an organization to be in charge during computer network attacks. In particular, SOLAR SUNRISE and exercise ELIGIBLE RECEIVER illustrated the lack of centralized control in DoD's response

Joint Chiefs decided in August 1998 to stand up a strong CND-JTF to be "in charge" during attacks. The JTF would have authority to direct and coordinate the entire DoD defense. CSAF stressed the need for a strong, directive, operationally minded CND-JTF

A CND-JTF Working Group stood up with representatives from CINCs, Services, agencies, and the Joint Staff. The working group has developed a proposed Charter and CONOP to ensure the JTF is stood up by the SECDEF's deadline of NLT 30 December 1998

- AF/XOIW, as Air Force lead, has coordinated the AF position with Air Staff (primarily AF/SC, SAF/IG, and SAF/GCM), MAJCOMs, and AIA

DISCUSSION

Bottom Line: Air Force can accept the CND-JTF as currently planned. The Charter and CONOP are both acceptable, though there are still improvements to be made

Milestones: Tank, VTC, SECDEF, IOC, FOC

Coordination for critical CND-JTF documents is nearing completion

- Charter has finished final coordination and will be released after the 21 October Tank

- CONOP has just begun its second round of coordination; comments are due back on 26 October. The third and last round will be from 30 October to 9 November

Major remaining action for AF is to define the component force, the AFFOR. Although J-39 has not pressed the services with any deadline, many seniors want the issue decided quickly. The Joint Staff will likely raise the issue during the SECDEF brief on 30 October.

- Navy and Army both likely to name their communications commands (NAVTELCOM and Army Signal Command) as component force. Doesn't meet early expectations that Service CERTs would be assigned

Capt Healey/AF/XOIWD/697-8701/14 October 1998

- Headquarters Air Force still needs to decide how the AFFOR should be composed. The two key pieces will be AFCERT and AFNOC (the Network Operations Center at Gunter AFB, GA). The likely COMAFFOR will be AFIWC/CC

AF comments on both Charter and CONOP have been accepted with three main exceptions

- CND-JTF will not have any LE or CI personnel on its staff, instead relying on DISA GOSC expertise. SAF/IGX and GCM have both stressed the importance of having full-time JTF LE and CI support. OSD/C3I has also made the comment. J-39 has non-concurred, wanting to keep the JTF as lean as possible.

- As noted, CND-JTF will rely for LE expertise on DISA GOSC, which has assigned special agents from the Defense Criminal Investigative Service. Almost the entire rest of the LE community does not want DCIS to be involved in computer LE investigations, preferring the JTF go to the Services. J-39 is willing to let the JTF work with DCIS.

- CND-JTF will not have a full-time lawyer on its staff, instead relying on DISA GC. According to SAF/GCM, not only should there be a full-time lawyer on the JTF, it should be a Staff Judge Advocate rather than a GC. SJAs are the correct type of support for an operational commander and can give advice on topics, such as rules of engagement, that GCs are not entitled to give

Personnel issues have been some of the most rancorous ones in the JTF working group. There are three key issues here:

- Comm-computer officers or operators? The mix of comm-computer officers and operators in the JTF has been a major area of disagreement. The CND-JTF will be staffed mostly by traditional operators (pilots, combat arms, etc.), relying on DISA for technical comm-computer expertise. Additionally, the Commander is an AF two-star fighter pilot, Maj Gen Campbell. Altogether, this matches CSAF's wishes for an operationally minded JTF

- Service Equity. Navy has non-concurred with the Charter, since an AF general has been named as commander and an AF colonel (Col Rhoads from J-39) nominated for the deputy commander. Navy proposes a change to the Charter, specifying these top two positions must not be same service. This means Navy will start with the deputy slot, which they are prepared to fill with their FIWC commander. J-39 is proposing several ways to get around this impasse. Most any solution should be acceptable to AF

- Services must provide names of the initial ten cadre members by 26 October. AF must provide two names: one is already tentatively identified, leaving one 14N

CND-JTF, according to the draft CONOP, will direct defensive actions to its component forces at INFOCON BRAVO or higher. It may coordinate defensive actions against any strategic attack (that is, an attack that crosses CINC/Service/Agency borders or for any attack with widespread or critical effects).

- Director, DISA and Director, Joint Staff have discussed the issue, however, and feel the JTF needs more “day-to-day control” of its components. Air Force can likely live with this, if control is limited to strategic attacks, and not AF-only incidents

- CINCs have been very protective their privileges, and see JTF direction of CINC network defenses as akin to meddling in their theater. As currently written, however, the Charter leaves a loophole for JTF directive authority to the CINCs, though this would likely rarely be used

Scope of CND-JTF has occasionally threatened to break out of just CND and into broader information assurance. In particular J-6 and DISA members of the working group have tried to strengthen the JTF’s role in red teaming, vulnerability assessments, and assuring network security *before an actual attack*. While these are critical functions to assure the security of our networks, they are not part of the JTF’s computer network warfighting role and have been strongly resisted by the Services.

RECOMMENDATION:
CND-JTF is nearing completion and will be a strong, directive, operationally minded organization. Air Force can accept the CND-JTF in its curr