CND-JTF Update

Capt Jay Healey
AF/XOIWD

Bottom Line

- CND-JTF 80% to 90% complete
- Air Force *cannot* accept the CND-JTF as currently envisioned
  - Remaining critical issue is LE/CI coordination
  - All other issues are acceptable

Overview

- CND-JTF at a Glance
- Hot Issues
- Determining AFFOR

CND-JTF Background

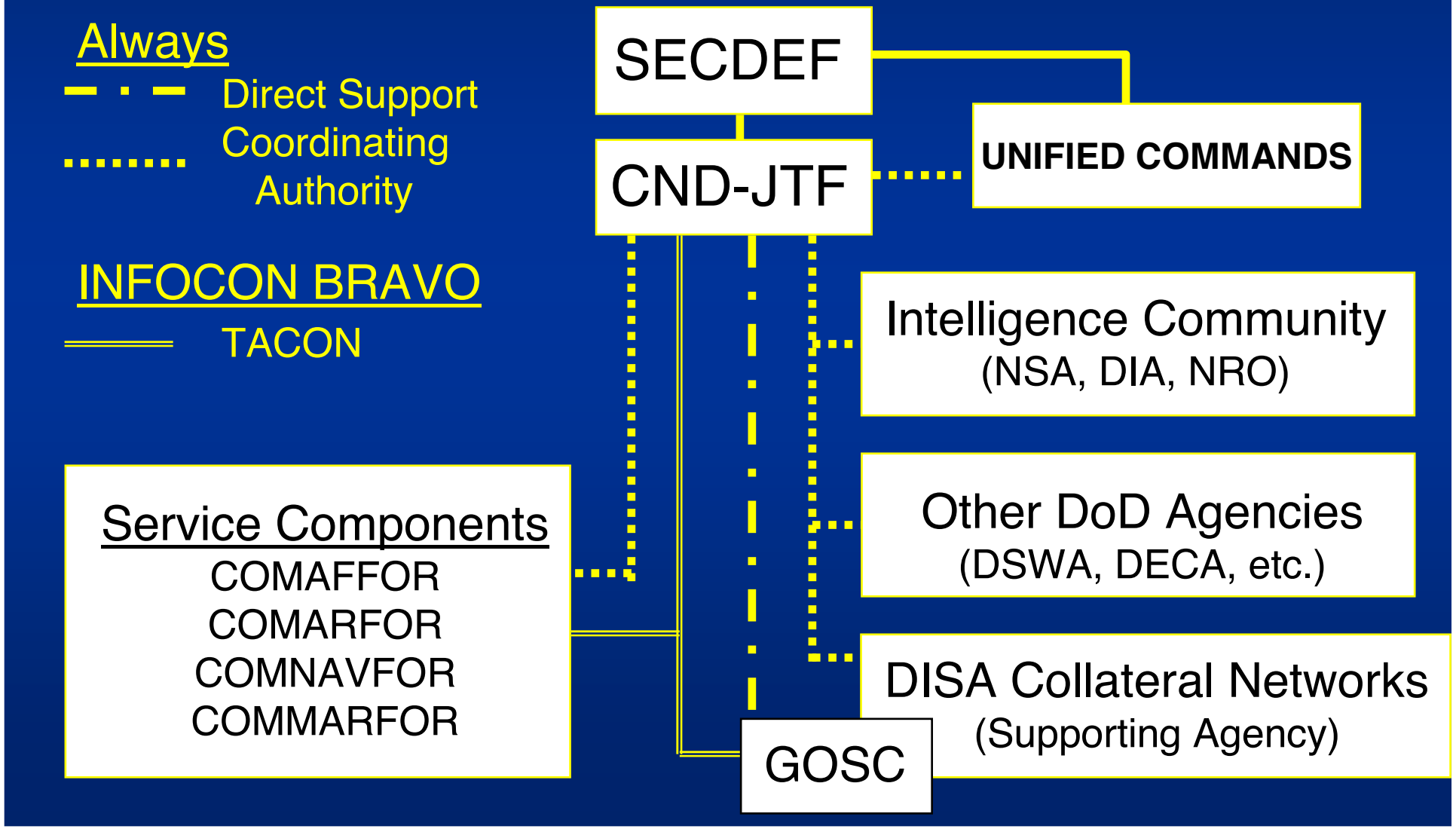
- CND-JTF will direct and coordinate DoD reaction to compunter network attacks (CNA)
  - Commander will be Maj Gen Campbell
- Will have component forces from Services for two key CND functions
  - Detecting and assessing CNA
  - Recommending countermeasures and restoring networks post-CNA
- AF must determine component force (AFFOR) and commander (COMAFFOR)

CONOPs in a Nutshell

- CND-JTF will
  - Monitor incidents, operations, vulnerabilities, intel threats
    - Leverage Intrusion Detection/Advisory Compliance System
  - Coordinate and Direct actions to stop/contain attacks
  - Perform Attack Assessments
  - Develop Intel Requirements for CND
  - Develop Plans & procedures to protect DoD networks
  - Participate in joint training exercises

- CND-JTF will not initiate offensive action

CND-JTF C2 Relationships



Timeline

- 15 to 26 Oct - Second CONOP coordination
- 20 Oct - VTC with CINCs (O-6 level)
- 21 Oct - OPSDEPs Tank for progress review
- 25 Oct - Charter to SECDEF for signature
- 26 Oct - AF must name initial cadre to Joint Staff
- 30 Oct - SECDEF progress review
- 30 Oct to 9 Nov - Final CONOP coordination
- NLT 30 Dec - IOC
- IOC + 180 days - FOC

Overview

- CND-JTF at a Glance
- Hot Issues
- Determining AFFOR

Outstanding AF Comments

- CND-JTF must have full-time legal support (instead of borrowing DISA's). Also, support must be SJA not GC.
  SAF/GCM
  SAF/IGX
  Army Concurs
- CND-JTF must have full-time law enforcement and counterintelligence
  SAF/GCM
  SAF/IGX
  ASD/C3I Concurs
- CND-JTF must not rely on DISA GOSC's law enforcement personnel; use Services instead
  SAF/GCM
  SAF/IGX
  Navy Concurs

Personnel Issues

- JTF predominantly manned by traditional operators -- will rely on DISA for much of its technical expertise
- Commander, deputy may both be AF causing Navy to non-concur
- Services must give names of initial cadre to Joint Staff NLT 26 Oct

Directive Authority

- Per draft CONOP, CND-JTF will have directive authority over component forces at INFOCON BRAVO
  - BRAVO: significant levels of probes/scans, targeting of specific DoD entity, or attacks with no impact on DoD operations
- JTF will have coordination authority only over CINC defensive actions
- Navy has resisted <u>any</u> JTF directive authority

Overview

- CND-JTF at a Glance
- Hot Issues
- Determining AFFOR

Needed AFFOR Capabilities

Per Draft CND-JTF CONOP

- Notify CND-JTF of attacks
- Conduct preliminary attack assessments
- Recommend attack countermeasures
- Restore/Maintain networks after attacks
- Provide network status
- Correlate incidents
- Provide status of ongong investigations

Critical Capabilities

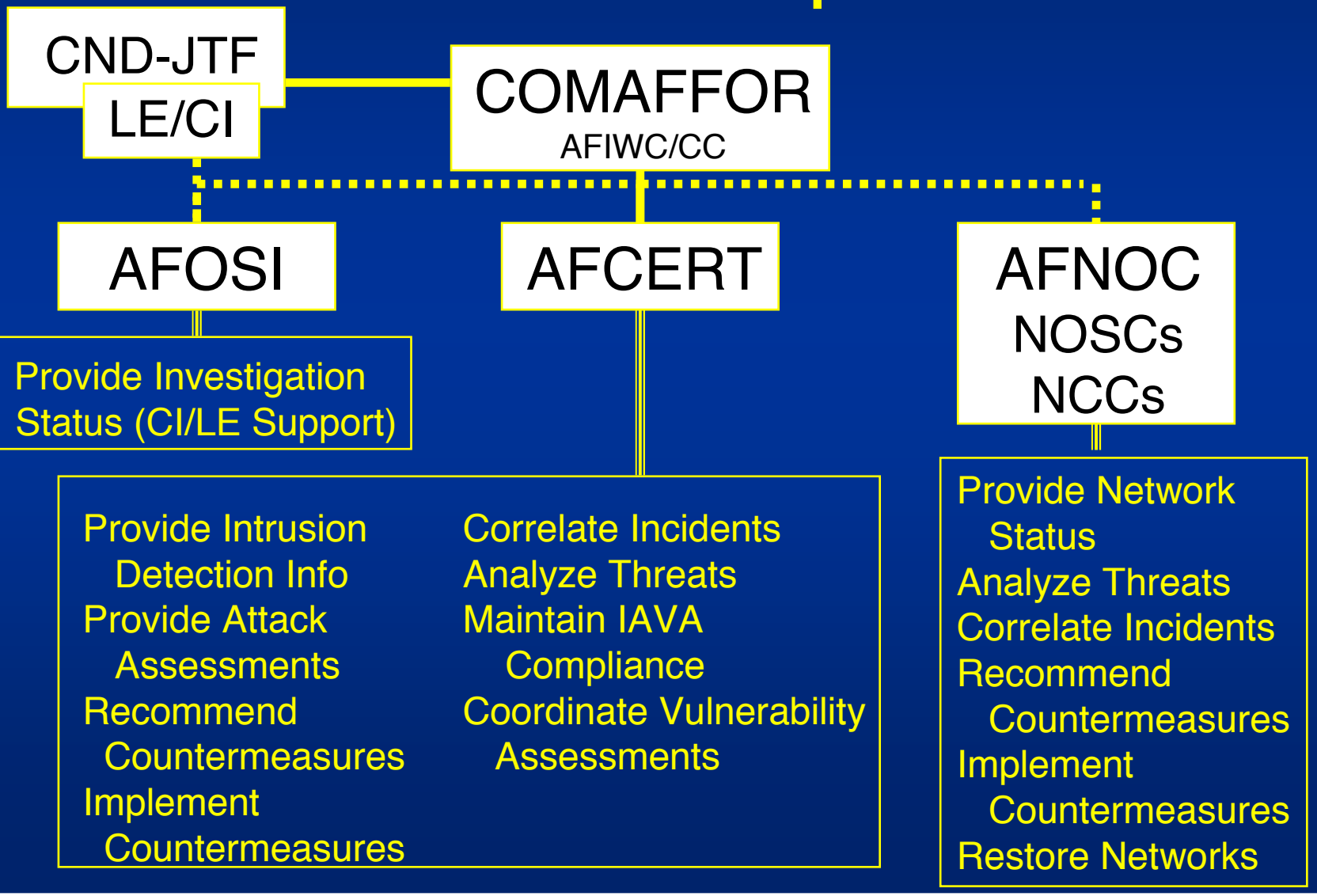
- Perform Vulnerability Analysis and Assistance Program
- Maintain IAVA compliance
- Analyze threats to Service networks
- Coordinate vulnerability assessments
- Conduct 24 x 7 ops
- Execute C2 IAW CONOP

Other Service Approaches

- COMARFOR: Army Signal Command
  - ARFOR: Combination of ASC and LIWA
- COMNAVFOR: Navy Telecommunications Command
  - NAVFOR: Combination of NAVTELCOM and FIWC

AFFOR Need Not Match other Service Components
AFCERT more capable than other CERTs
Meets more needed component capabilities
CND-JTF Expected CERTs as Service Components

Proposed AFFOR Relationships



Backup Slides

JTF Manpower

AF Billets

- Intel Analyst (O4, 14N) Cadre
- Def IO Officer (O4, 33SX)
- Watch Officer (O4, 13SX) Cadre
- Def IO Planner (O4, 11XX)

- Commander (O-8)
- Dep Cmdr (O-6) (Nominated)

Billets by Specialty

- Operators: 10 of 19
- Comm: 4 of 19
- Intel: 5 of 19

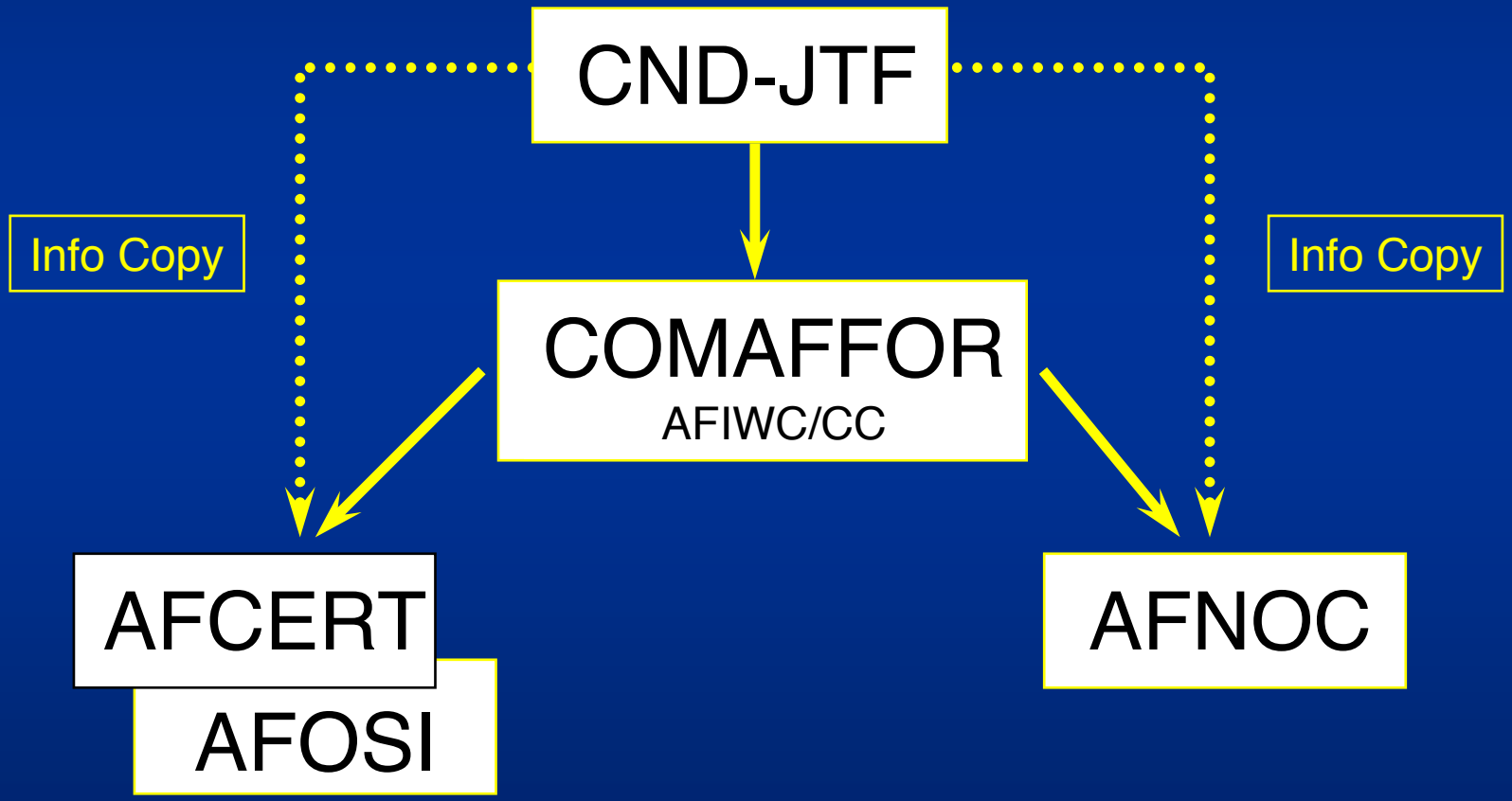
Service Totals

- USAF: 4 (+ 2)
- USA: 6
- USN: 5
- USMC: 2

Doctrinal Basis for AFFOR
AFDD 2-5

- AFDD 2-5: "… successful military operations must carefully integrate both OCI and DCI elements."
- AFDD 2-5: "… AFCERT established as the single point of contact in the Air Force for computer security incidents and vulnerabilities. The AFCERT coordinates the AFIWC's techical resources to assess, analyze, and provide countermeasures for computer security incidents and vulnerabilities reported [by] Network Control Centers, IWS, and NOSC."

AFFOR Tasking Flow



JTF-CND Update

- JTF will direct/coordinate DoD computer defenses
  - JTF Paperwork 90% Complete; IOC no later than 30 Dec 98
- IC very protective of intel networks, DCI authorities
  - IC will submit to JTF coordination authority as well as report network status and incidents to JTF
  - JTF and CMS will undertake MOA on specifics
- JTF purposefully lean ... J2 cell only 5 people
  - Will generate PIRs, monitor I&W, help analyze specific attacks. Must depend on remainder of IC for all else
  - AF has one O-4 in the J2; exact person still TBD
- AF has one outstanding issue
  - JTF must have full-time body for LE/CI coordination