DOD Organization for Computer Network Defense

Summary of Proposals

June 1998

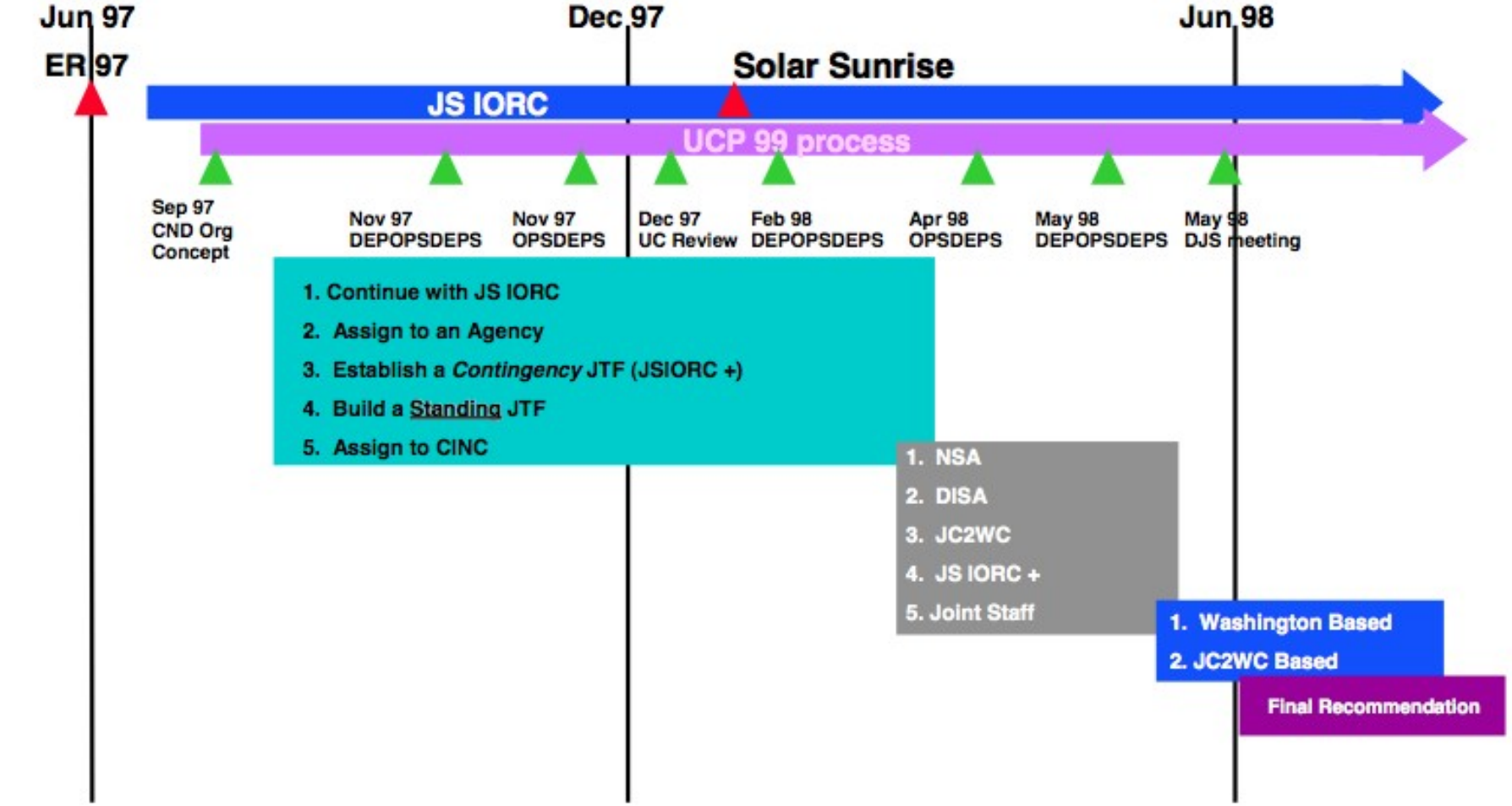
Purpose

To provide a summary of the proposals for an *interim* organizational structure that can coordinate and direct the defense of DOD Computer Networks and Systems until superseded by a long - term solution

Completed / Requested Actions

- [x] **DEPOPSDEPS:** ***Review brief to be presented to OPSDEPS***
- [x] **OPSDEPS:**
  - ***Conceptually approve organizational structure <u>options</u>***
  - ***Review brief to be presented to Unified Commands, reconvene to review comments and recommend option for CND structure***
- [x] **Unified Commands:** ***Provide comments / recommendations on VTC presentations***
- [x] **DEPOPSDEPS:** ***Approve recommended strategy for final option development***
- [x] **DJS Meeting:** ***Options reviewed, narrowed to two finalists***
- [x] **OPSDEPS:** ***Discuss final option for recommendation to JCS***
- [ ] **ACOM J3/5 Provide comments and recommendations**
- [ ] **Unified Commands: Provide comments**
- [ ] **JCS Tank:** ***Approve recommendation***

Evolution of Options



Results from 19 May DJS Meeting

- Representatives from each of the proposed organizations participated
- Consensus that this organization must plug into an umbrella organization which can, if required, be DOD focal point for coordination with National Infrastructure Protection Center
- Must still retain operational focus
- Narrowed to two options:
  - San Antonio-based JTF organized around JC2WC
  - Washington-based JTF (hybrid of previous proposals)
- Next step: OPSDEPS tank session

Proposed CND-JTF Mission

"Subject to the authority, direction, and control of the SECDEF, this organization will be responsible for coordinating and directing the defense of DOD computer systems and computer networks. This mission includes the coordination of DOD defensive actions with non - DOD government agencies and appropriate private organizations."

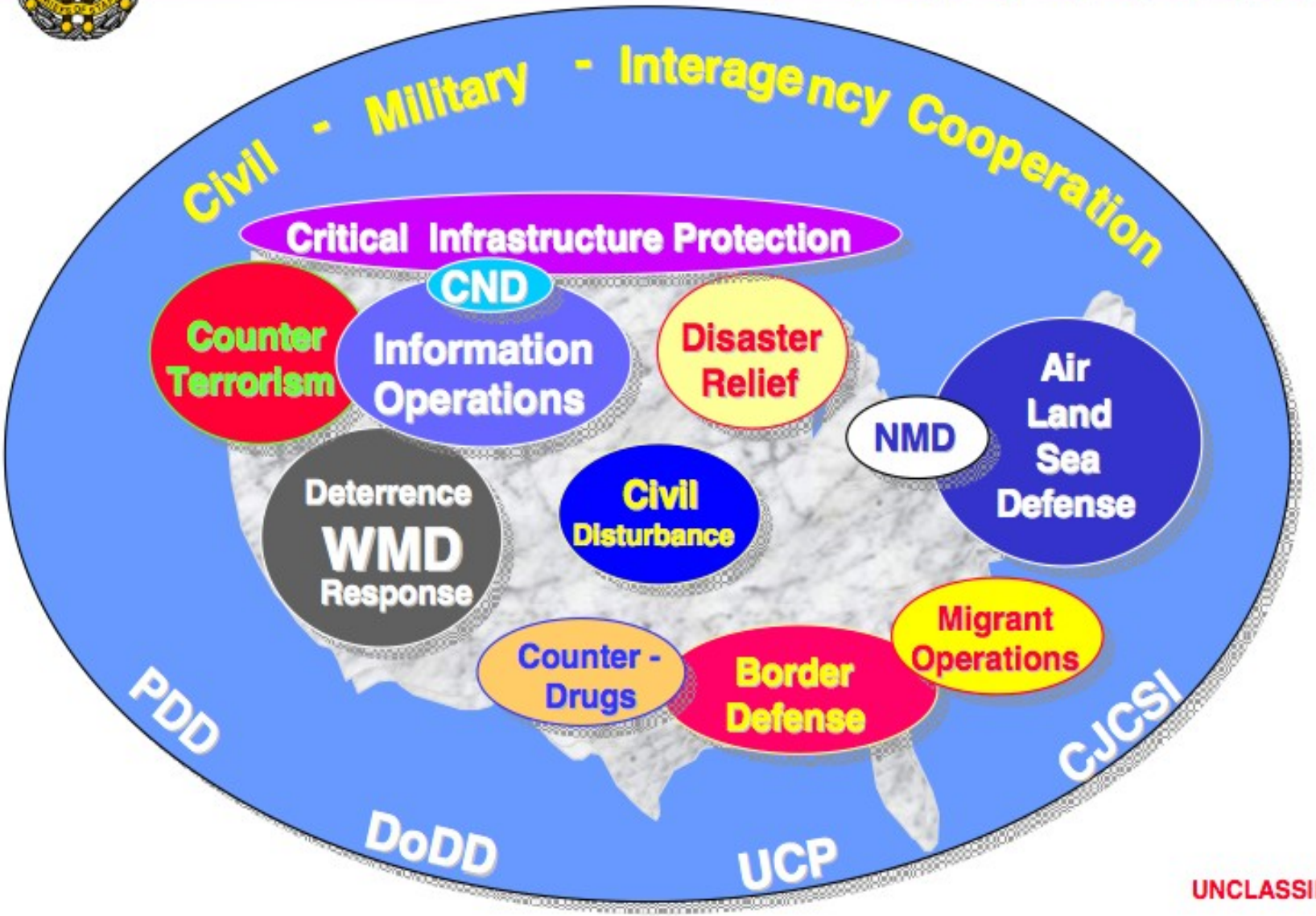
Specific Organizational Functions

- Organize, plan, and participate in joint training to conduct strategic CND
- Monitor Intelligence Community I & W reporting
- Provide Intelligence Community with PIR for collection and I & W requirements for potential attacks against DOD computers and networks
- Monitor status of DOD computer networks
- Determine when system(s) are under attack, assess operational impact, and notify NCA and user community
- Coordinate / direct appropriate DOD actions to stop attack, contain damage, restore functionality, and provide feedback to user community
- Coordinate with Defense - wide Information Assurance Program (DIAP) and Critical Asset Assurance Program (CAAP) authorities to ensure compliance with wider IA policy and initiatives
- Coordinate as required with NSC, NIPC, law enforcement agencies, other Interagency partners, private sector, and allies
- Assess effectiveness of defensive actions and maintain current assessment of operational impact on DOD
- Subject to authority, direction, and control of SECDEF, provide information to and receive direction from the CJCS, and provide liaison as required to the OSD staff and Joint Chiefs of Staff

Recent Guidance

- **Presidential Decision Directive 63 (22 May 98)**
  - **National Coordinator**
  - **National Infrastructure Protection Center (NIPC)**
  - **Department Implementation Plans w/in 180 days (ODUSD lead)**

Homeland Defense



Policy Issues

Info Operations
- CND first
- NIPC coordination

(*potential DoD equivalent to NIPC*)

Integration
- Active
- Reserve Component

STATUTORY
- Titles 10, 18, 32
- Int'l Agreements

UCP PROCESS

CONSEQUENCE MANAGEMENT
- SECARMY Executive Agent
- Revise DOD Policy Documents
- Revise Forces For Memo
- Interagency coordination

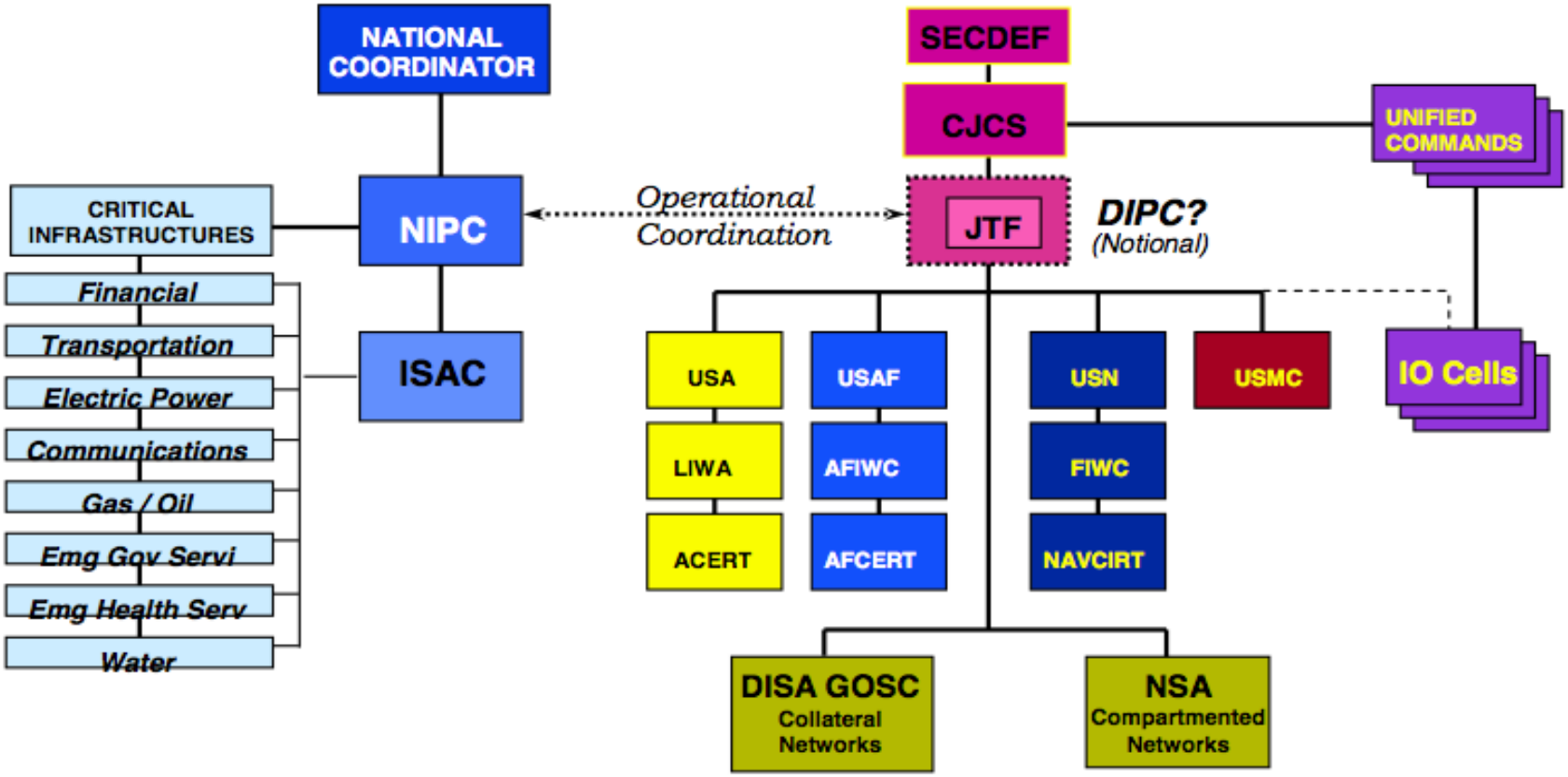
COMMAND STRUCTURES
- Counterdrugs JIATF / JTFs
- ACOM RTFs (includes CBIRFs, etc)
- Existing MOAs / MOUs
- SACLANT/ NORAD

UNCLASSIFIED

Operational Coordination

Inter-Agency

Department of Defense



JC2WC Proposal

CONCEPT :

- San Antonio based JTF leveraging existing relationships and personnel

REQUIREMENTS:

- Personnel
  - 23 JC2WC / 20 AFIWC billets
  - 9 additional personnel (requires reps from DISA, NAVCIRT, & ACERT)
- $5M start up / $3M recurring

JC2WC Proposal

CONCEPT :

- San Antonio based JTF leveraging existing relationships and personnel

REQUIREMENTS:

- Personnel
  - 23 JC2WC / 20 AFIWC billets
  - 9 additional personnel (requires reps from DISA, NAVCIRT, & ACERT)
- $5M start up / $3M recurring

PROS:

- Existing JC2WC relationships with CINCs
- Basic 24 x 7 Watch with AF support (AFIWC/AIA)
- Connectivity in-place now or programmed with Services and Agencies
- Available office / watch center space (AFIWC)
- Significant personnel commitment (20 AF / 23 JC2WC)
- Synergy of JC2WC / AIA / AFIWC co-location
- Quickest start-up: immediate cadre available

JC2WC Proposal

CONCEPT :

- San Antonio based JTF leveraging existing relationships and personnel

REQUIREMENTS:

- Personnel
  - 23 JC2WC / 20 AFIWC billets
  - 9 additional personnel (requires reps from DISA, NAVCIRT, & ACERT)
- $5M start up / $3M recurring

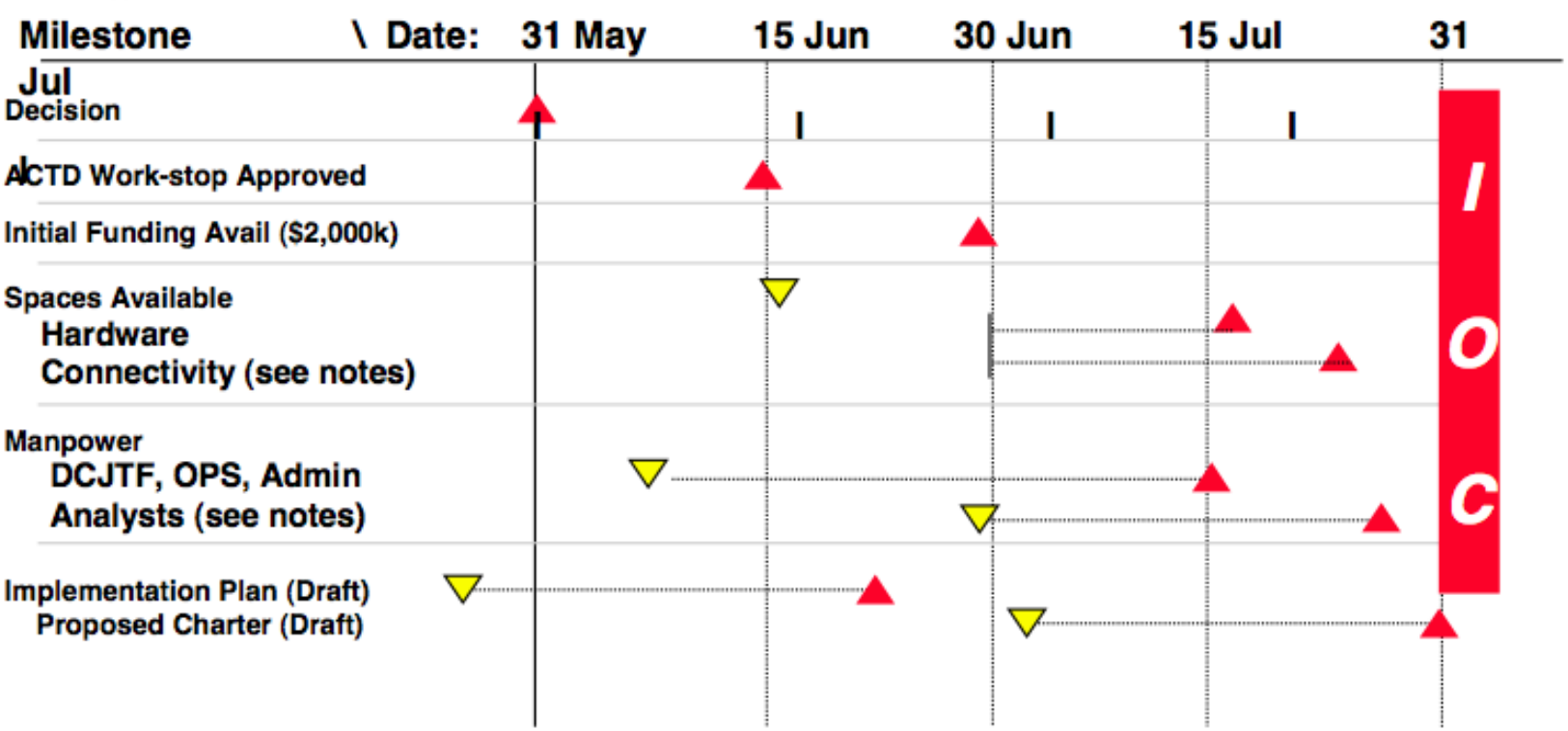
PROS:

- Existing JC2WC relationships with CINCs
- Basis 24 x 7 Watch with AF support (AFIWC/AIA)
- Connectivity in-place now or programmed with Services and Agencies
- Available office / watch center space (AFIWC)
- Significant personnel commitment (20 AF / 23 JC2WC)
- Synergy of JC2WC / AIA / AFIWC co-location
- Quickest start-up: immediate cadre available

CONS:

- Washington DC detachment required for interagency coordination
- JC2WC support for OSD ACTDs impacted: need to transfer responsibility or backfill JC2WC billets to maintain ACTD support capability
- Minimal (baseline) operational capability; some surge capability

JC2WC IOC Milestones



Initial Operational Capability (31 July 1998) defined as baseline correlation, analysis, reporting and monitoring / coordinating incident response activities. Initial operations will be less than continuous 24 x 7 due to manpower availability, skill levels, and additional requirements associated with stand-up of the JTF (developing policy / doctrine guidance, coordination with other CERTs / agencies). Early operations will leverage off current AFCERT and AIA / IOC activities (co-located) but virtual and physical representation of NAVCIRT/ ACERT / DISA network status is required at IOC. Expanded capabilities available at follow-on intervals based on manpower availability and skills, space and hardware procurement, connectivity, and funding.

JTF Impact On Current JC2WC Mission

- **Current Mission Area Trade-Offs**
  - **Assessing ACTD IO Vulnerabilities (5 billets); *tasked by OSD/C3I***
  - **Executing ACTD and other technology demonstrations (13 billets); *tasked in the current JC2WC charter***
- **Impact of mission deletion**
  - **OSD will have to transfer analytical vulnerabilities responsibilities elsewhere**
  - **The Joint honest broker bridge between CINCS and the R&D community will be severed for ACTD and technology demonstration**
- ***May be able to cover some of these impacts in ACOM transfer . . .we should be willing to backfill where required***

JC2WC Proposal

JC2WC/CC

Deputy CJTF 1
Admin 1

SJA / PAO ** 2

Total:	**52**
JC2WC:	**23**
AIA:	**20**
TBD:	**9**

DC Det

Dep CJTF	#
OIC	1
OPS	3
Intel	1
Plans	2
IOTC	1
JWAC	1
ADMIN	1
TOT	10

Operations

Watch Commander	5
Watch NCO / OPS Analysts	5
Network Analysts / DISA	5 @
AFCERT Analyst (NAVCIRT) (ACERT)	5
Law Enforcement	5
TOT	25

Intelligence

Chief	1
Analyst	5
TOT	6

Plans

Counter Off	3
Counter Off	2
Network Resp	2
TOT	7

** USAF will source
@ Contractors
# Will deploy from SA as required.

NOTE: 43 of the 52 billets are currently at San Antonio

Washington-Based Proposal

CONCEPT

- Washington-based JTF; synthesis of previous proposals
- Based within DISA facilities but not part of DISA
  - Capitalize on synergies of DISA co-location
  - DISA provides facility, connectivity, synergy, some personnel, and support for JTF

REQUIREMENTS

- 29 Personnel (4 from DISA)
- Minimal $3M start-up, $2M recurring

Washington-Based Proposal

CONCEPT

- Washington-based JTF; synthesis of previous proposals
- Based within DISA facilities but not part of DISA
  - Capitalize on synergies of DISA co-location
  - DISA provides facility, connectivity, synergy, some personnel, and support for JTF

REQUIREMENTS

- 29 Personnel (4 from DISA)
- Minimal $3M start-up, $2M recurring

PROS

- **Resident CND capability (ASSIST, DIAMOND, R & D)**
- **Basic 24 x 7 Watch with DISA support**
- **Global network management infrastructure**
- **Established relationships with CINCs, DOD, and Interagency activities**
- **Available office / watch center space**
- **Connectivity in - place now or programmed**

Washington-Based Proposal

CONCEPT

- Washington-based JTF; synthesis of previous proposals
- Based within DISA facilities but not part of DISA
  - Capitalize on synergies of DISA co-location
  - DISA provides facility, connectivity, synergy, some personnel, and support for JTF

REQUIREMENTS

- 29 Personnel (4 from DISA)
- Minimal $3M start-up, $2M recurring

PROS

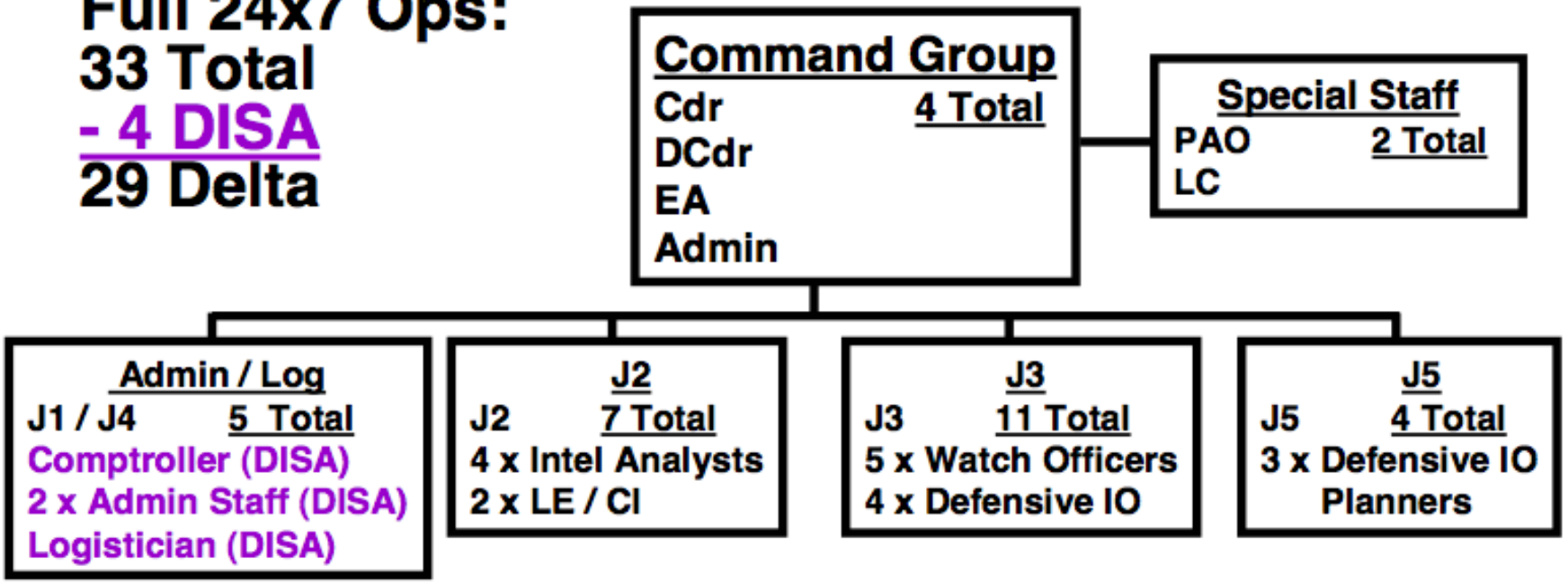
- Resident CND capability (ASSIST, DIAMOND, R & D)
- Basic 24 x 7 Watch with DISA support
- Global network management infrastructure
- Established relationships with CINCs, DOD, and Interagency activities
- Available office / watch center space
- Connectivity in - place now or programmed

CONS

- **Significant manpower requirement**
- **Start-up time TBD: no personnel identified**
- **Minimal (baseline) operational capability; no surge capability**

Washington-Based Proposal

Full 24x7 Ops:
33 Total
- 4 DISA
29 Delta



JTF Resource Matrix

	JC2WC	DC-based
Personnel Provided	52 43	33 4
Comms needed	yes	yes
Facility needed	no AFIWC	no DISA
Start-up Costs	$5M	$3M
Recurring Costs	$3M	$2M

Recommendation

OPSDEPS endorse JC2WC-based option as best interim organization to direct Computer Network Defense for DOD.

Way - Ahead

- **Meet with ACOM to discuss JC2WC proposal**
- **VTC with Unified Commands for comment**
- **Present at JCS Tank for final approval**