

CND-JTF AFFOR

Capt Jay Healey
AF/XOIWD



Purpose

To Determine the AF Component Force to the Computer Network Defense-Joint Task Force



CND-JTF Background

- CND-JTF will direct and coordinate DoD reaction to compunter network attacks (CNA)
- 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)



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

- 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

Critical Capabilities



AFNOC and AFCERT Who Does What?

AFNOC

- Central point for maintaining and running
 AF networks
- Blocks IPs at router per
 AFCERT recommenation
- Existing GOSC ties for network operations and information assurance

AFCERT

- Single AF POC for computer network defense
- Largest DoD intrusion detection network ... existing GOSC ties
- Recommends IP blocking to AFNOC
- Issues advisories and tracks compliance
- Coordinates LE and CI responses with OSI



AFNOC's AFFOR Functions

- Recommend CNA countermeasures -- Shared with AFCERT
- Restore/Maintain networks after CNA
- Provide network status
- Conduct 24 x 7 ops -- Shared with AFCERT
- Correlate incidents -- Shared with AFCERT
- Execute C2 IAW CONOP -- Shared with AFCERT
- Analyze threats to Service networks -- Shared with AFCERT



AFCERT's AFFOR Functions

- Notify CND-JTF of CNA incidents
- Conduct preliminary attack assessments
- Recommend CNA countermeasures -- Shared with AFNOC
- Conduct 24 x 7 ops -- Shared with AFNOC
- Correlate incidents -- Shared with AFNOC
- Execute C2 IAW CONOP -- Shared with AFNOC
- Provide status of ongong investigations
- Perform Vulnerability Analysis and Assistance Program
- Maintain IAVA compliance
- Analyze threats to Service networks -- Shared with AFNOC
- Coordinate vulnerability assessments

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



Doctrinal Basis for AFFOR AFDD 2-5

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



AFIWC as AFFOC Pros and Cons

- Pros:
 - AFCERT has ties to OSI, NIPC, DISA GOSC and ASSIST, and AFNOC
 - AFIWC brings full-spectrum IO for when JTF expands to all IW
 - AFNOC only brings info assurance
 - Best doctrinal fit
- Con: Does not perform network actions



AFNOC as AFFOR Pros and Cons

- Pros:
 - Center of AF info assurance
 - Tremendous comm-computer expertise
- Cons:
 - Only performs network actions
 - No ties to full-spectrum IW or LE/CI



Recommendation

- COMAFFOR: Commander, AFIWC
 AFFOR:
 - AFCERT for detection, assessments, etc.
 - AFNOC for corrective network actions

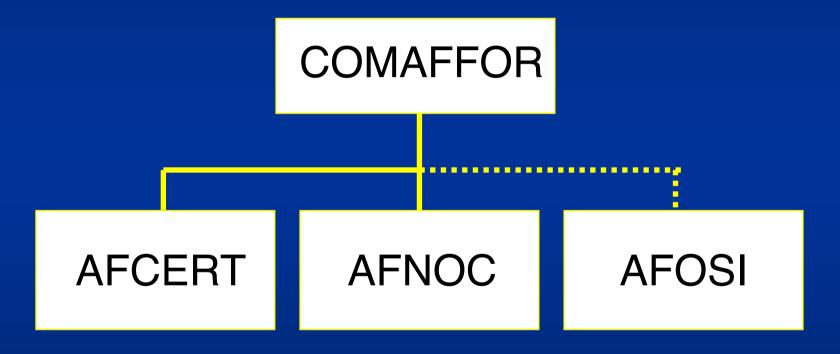
AFIWC/CC as COMAFFOR sets stage for potential full spectrum IW JTF at USSPACE



Backup Slides



AF Relationships





This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu