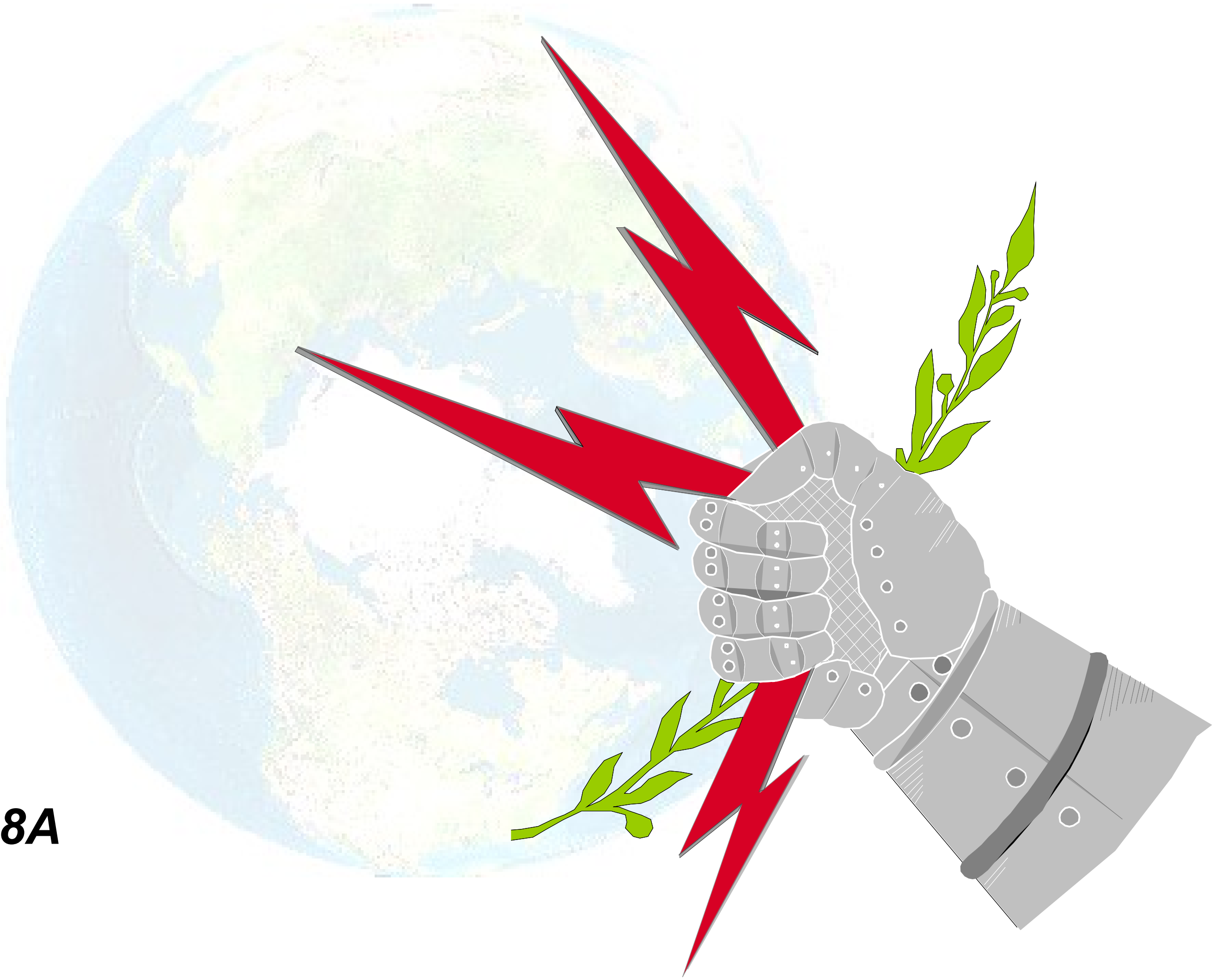
USSTRATCOM & DoD’S EFFORTS TO COMBAT CYBERTHREATS

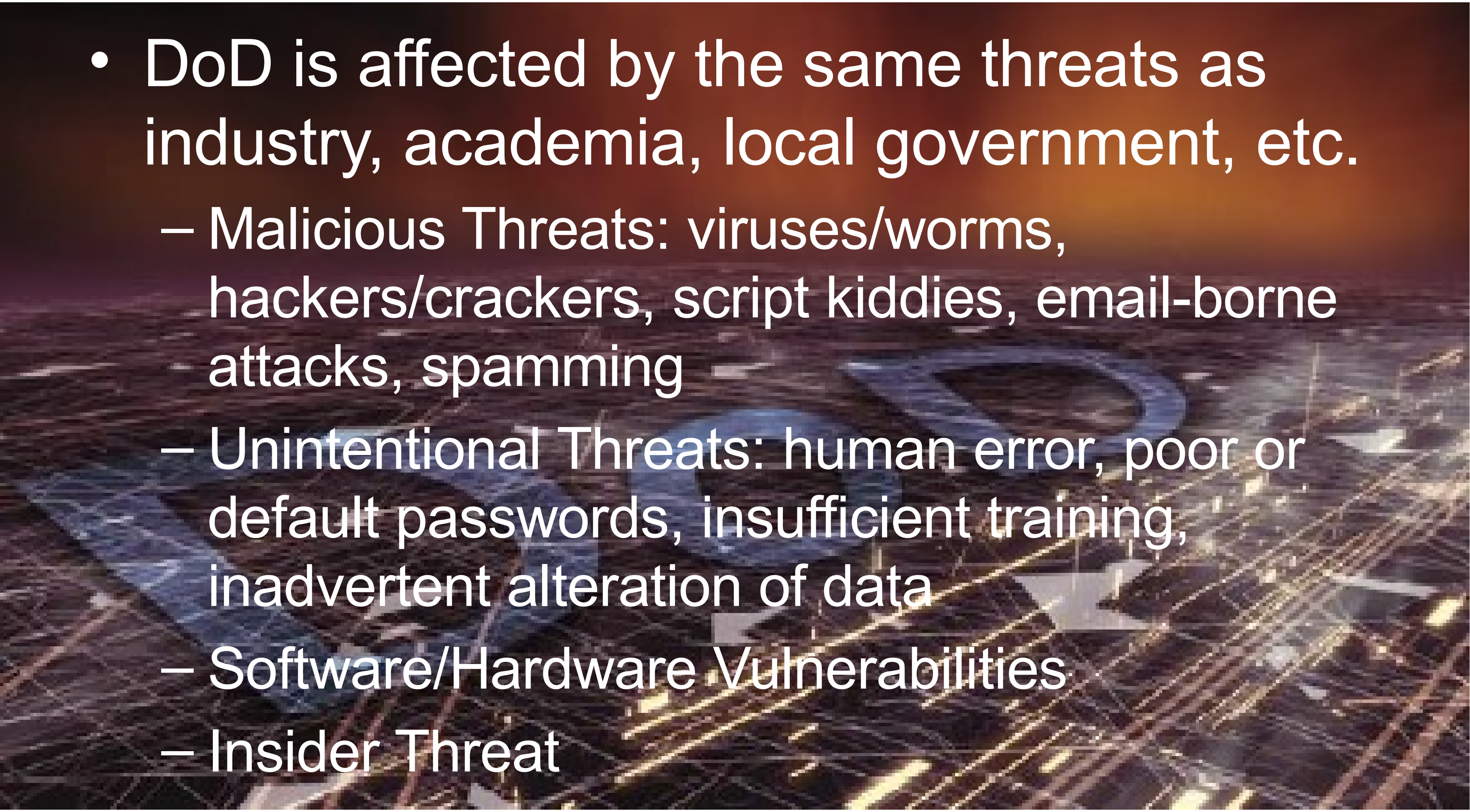


Mike Gipson
USSTRATCOM/J8A
10 August 2006

Agenda

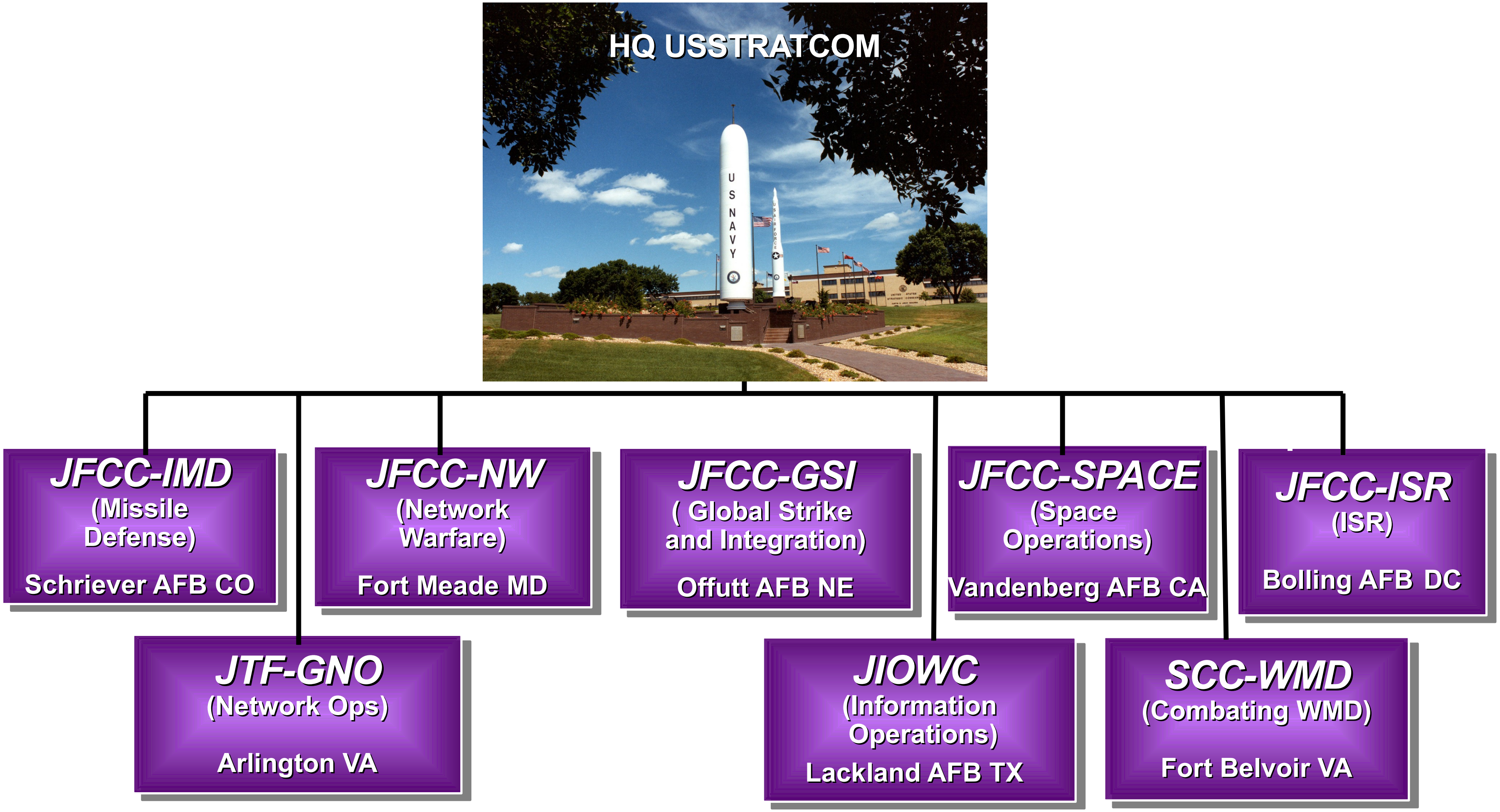
- Common Threats
- Organized to Combat the Threat
- DoD Enterprise-wide IA & CND Solutions Steering Group (ESSG)
- DoD-wide Accomplishments
- Way Ahead
- Summary

Common Threats



- DoD is affected by the same threats as industry, academia, local government, etc.
  - Malicious Threats: viruses/worms, hackers/crackers, script kiddies, email-borne attacks, spamming
  - Unintentional Threats: human error, poor or default passwords, insufficient training, inadvertent alteration of data
  - Software/Hardware Vulnerabilities
  - Insider Threat

Organized to Combat the Threat



HQ USSTRATCOM

JFCC-IMD
(Missile Defense)
Schriever AFB CO

JFCC-NW
(Network Warfare)
Fort Meade MD

JFCC-GSI
(Global Strike and Integration)
Offutt AFB NE

JFCC-SPACE
(Space Operations)
Vandenberg AFB CA

JFCC-ISR
(ISR)
Bolling AFB DC

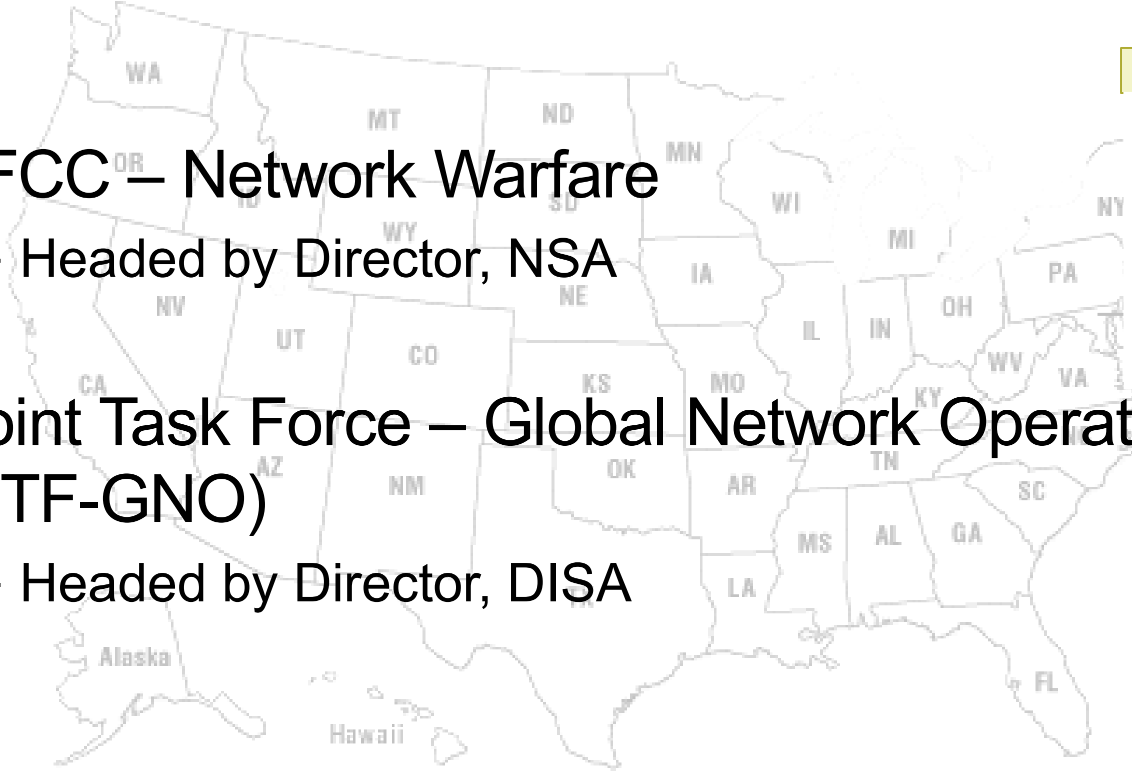
JTF-GNO
(Network Ops)
Arlington VA

JIOWC
(Information Operations)
Lackland AFB TX

SCC-WMD
(Combating WMD)
Fort Belvoir VA

The Tip of the Spear

JFCC-NW (Ft Meade MD)
JTF-GNO (Arlington VA)



- JFCC – Network Warfare
  - Headed by Director, NSA
- Joint Task Force – Global Network Operations (JTF-GNO)
  - Headed by Director, DISA

LTG Alexander

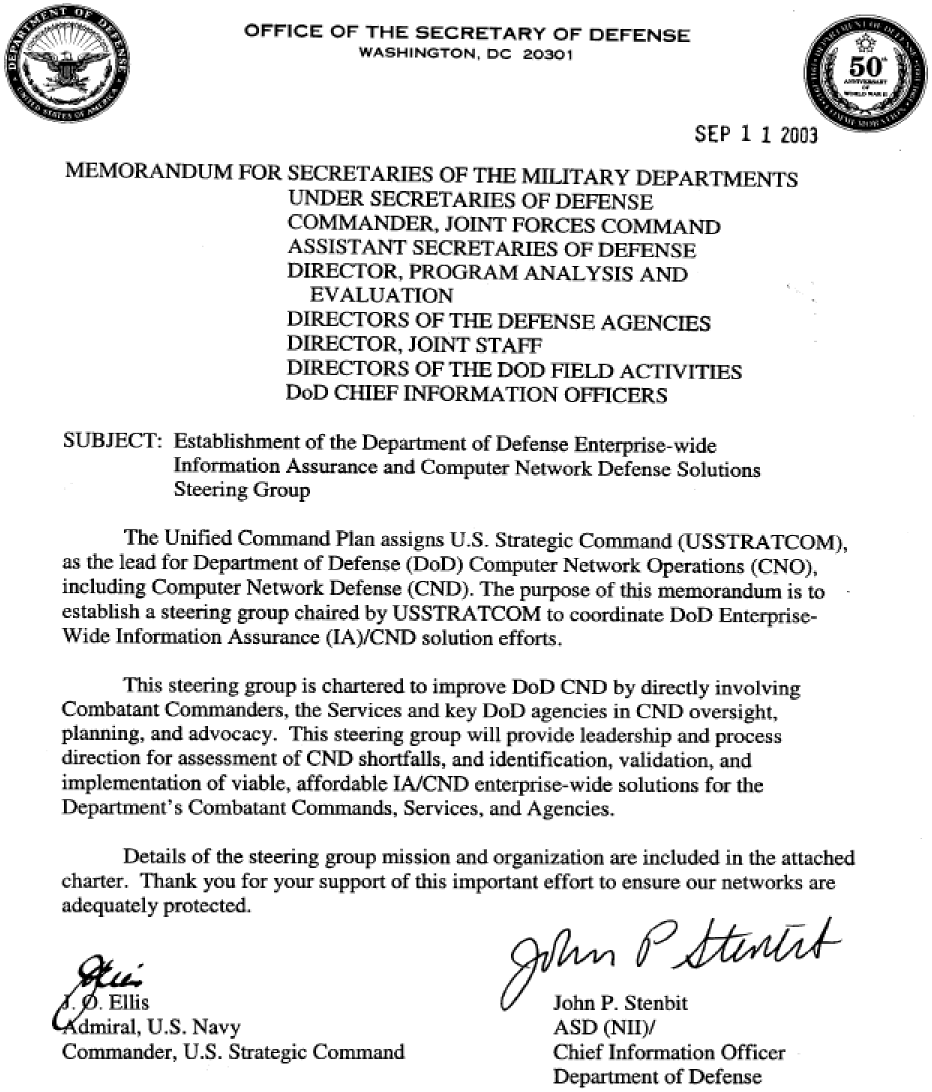
Lt Gen Croom

Collaborative Efforts

- Implementing event and incident correlation databases at CERT facilities
- Strengthening JTF-GNO Operational Support
- Standardizing ND tools, capabilities & practices (ESSG)

- Provide battlespace visibility & situational awareness
- Identify attack impacts
- Consequence management & response
- Course of action development

DoD Enterprise-wide IA and CND Solutions Steering Group (ESSG)



OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC 20301

SEP 1 1 2003

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
UNDER SECRETARIES OF DEFENSE
COMMANDER, JOINT FORCES COMMAND
ASSISTANT SECRETARIES OF DEFENSE
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, JOINT STAFF
DIRECTORS OF THE DOD FIELD ACTIVITIES
DoD CHIEF INFORMATION OFFICERS

SUBJECT: Establishment of the Department of Defense Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group

The Unified Command Plan assigns U.S. Strategic Command (USSTRATCOM), as the lead for Department of Defense (DoD) Computer Network Operations (CNO), including Computer Network Defense (CND). The purpose of this memorandum is to establish a steering group chaired by USSTRATCOM to coordinate DoD Enterprise-Wide Information Assurance (IA)/CND solution efforts.

This steering group is chartered to improve DoD CND by directly involving Combatant Commanders, the Services and key DoD agencies in CND oversight, planning, and advocacy. This steering group will provide leadership and process direction for assessment of CND shortfalls, and identification, validation, and implementation of viable, affordable IA/CND enterprise-wide solutions for the Department's Combatant Commands, Services, and Agencies.

Details of the steering group mission and organization are included in the attached charter. Thank you for your support of this important effort to ensure our networks are adequately protected.

J. O. Ellis
Admiral, U.S. Navy
Commander, U.S. Strategic Command

John P Stenbit
John P. Stenbit
ASD (NII)/
Chief Information Officer
Department of Defense

Co-Chaired by USSTRATCOM and JTF-GNO.

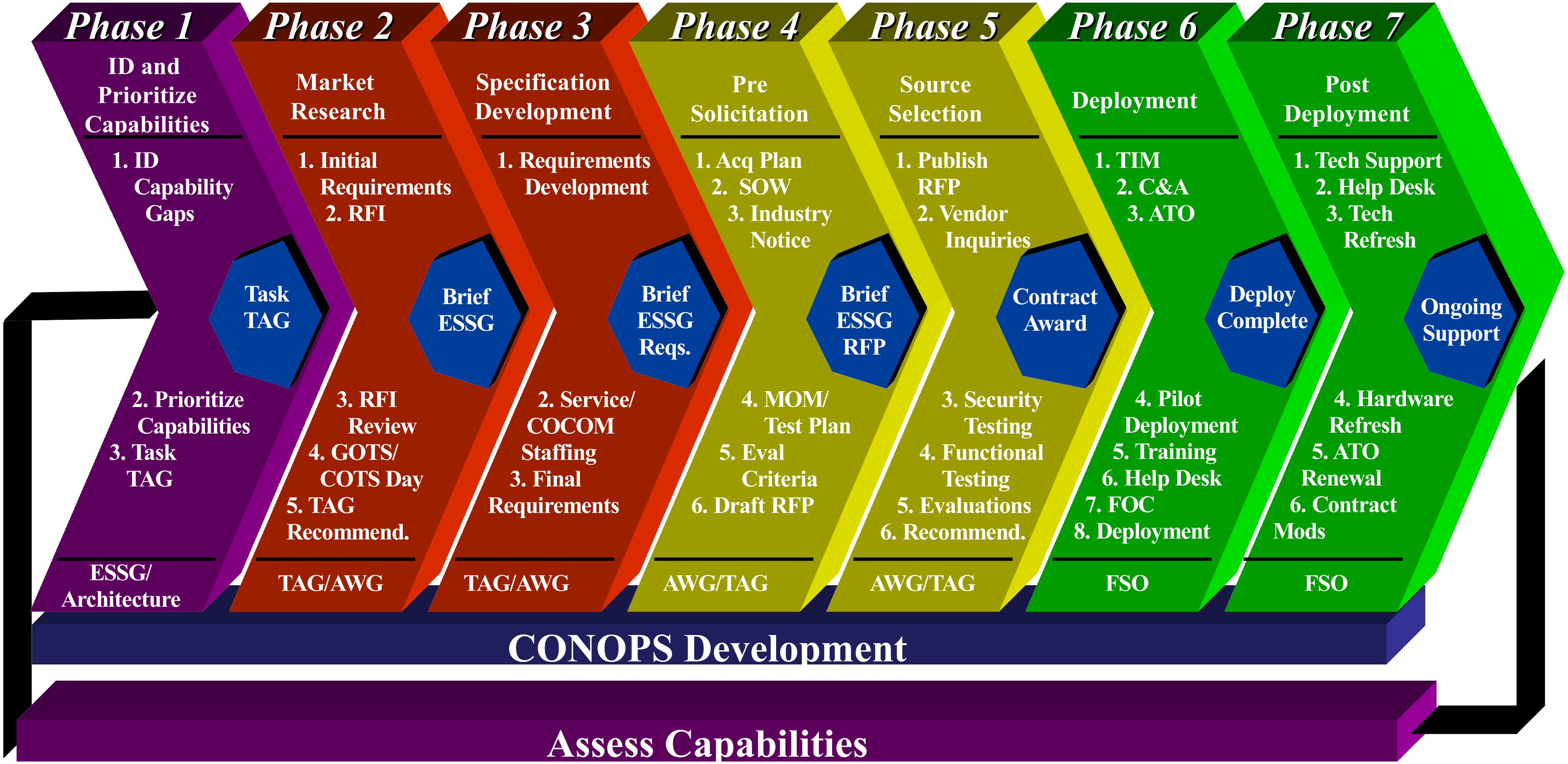
Improve CND by directly involving CC/S/As in CND oversight, planning, and advocacy.

Voting members include NSA, DIA, DISA, JS/J6, DIAP (OASD/NII), JFCOM, Services.

Assess shortfalls; identify, validate and implement viable, affordable enterprise-wide solutions.

Streamline acquisition process to make solutions available quickly.

ESSG Life Cycle Model



Phase 1

ID and Prioritize Capabilities

1. ID Capability Gaps

Task TAG

2. Prioritize Capabilities
3. Task TAG

ESSG/ Architecture

Phase 2

Market Research

1. Initial Requirements
2. RFI

Brief ESSG

3. RFI Review
4. GOTS/ COTS Day
5. TAG Recommend.

TAG/AWG

Phase 3

Specification Development

1. Requirements Development

Brief ESSG Reqs.

2. Service/ COCOM Staffing
3. Final Requirements

TAG/AWG

Phase 4

Pre Solicitation

1. Acq Plan
2. SOW
3. Industry Notice

Brief ESSG RFP

4. MOM/ Test Plan
5. Eval Criteria
6. Draft RFP

AWG/TAG

Phase 5

Source Selection

1. Publish RFP
2. Vendor Inquiries

Contract Award

3. Security Testing
4. Functional Testing
5. Evaluations
6. Recommend.

AWG/TAG

Phase 6

Deployment

1. TIM
2. C&A
3. ATO

Deploy Complete

4. Pilot Deployment
5. Training
6. Help Desk
7. FOC
8. Deployment

FSO

Phase 7

Post Deployment

1. Tech Support
2. Help Desk
3. Tech Refresh

Ongoing Support

4. Hardware Refresh
5. ATO Renewal
6. Contract Mods

FSO

CONOPS Development

Assess Capabilities

Major ESSG Accomplishments

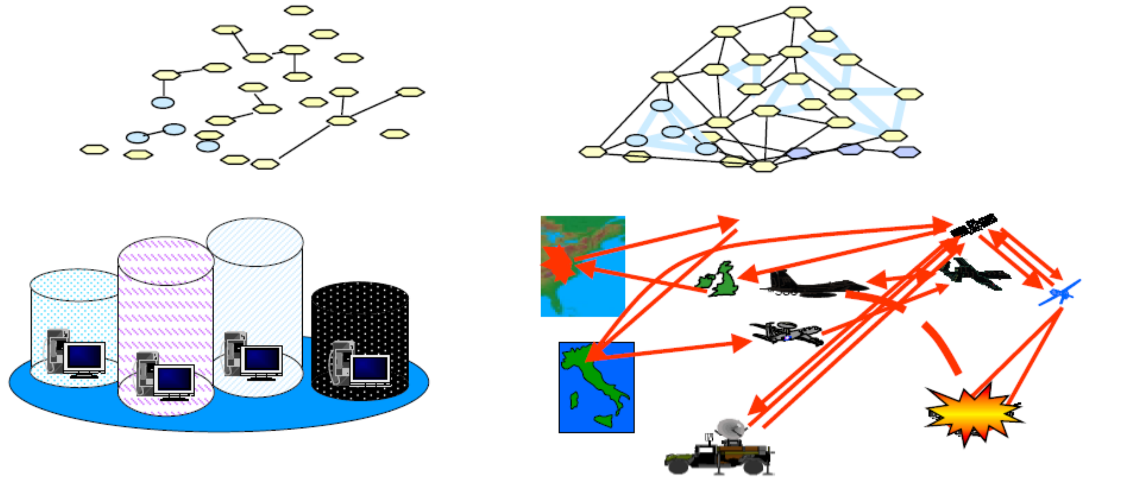
- Secured centralized funding for DoD Enterprise solutions
- Awarded DoD Enterprise-Wide contracts for:
  - **Vulnerability Management (VM) Scanning (SCCVI)**
  - **Automated Remediation/Patching (SCRI)**
  - **Anti-Adware/Spyware (SDEP)**
  - **Host-Based Centralized Management Capability and System Baselining Tool (HBSS)**
- Established formal requirements groups:
  - **Technical Advisory Group (TAG)**
  - **Acquisition Working Group (AWG)**
  - **CONOPS Working Group (CWG)**
  - **CND Architecture Working Group (ASG)**

ESSG Direction

- UDOP
- Wireless detection/IDS
- Insider Threat - Focused Observation Tool
- Tier 3 SIM

Way Ahead

- We must be able to collect information, then quickly and reliably share it with everyone who needs it
- This is accomplished through *Network Centric Operations* vice *Platform Centric Operations*



Platform-Centric

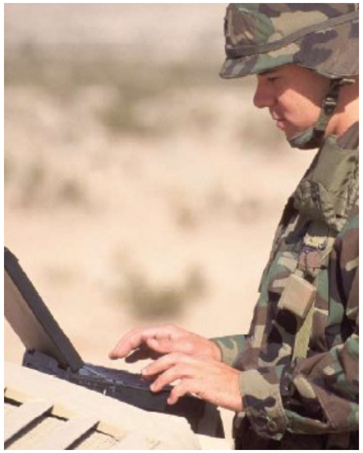
Network-Centric

Traditional stove-pipe approach

Fused information available on the net

Information Sharing Using STRATCOM'S SKI Web

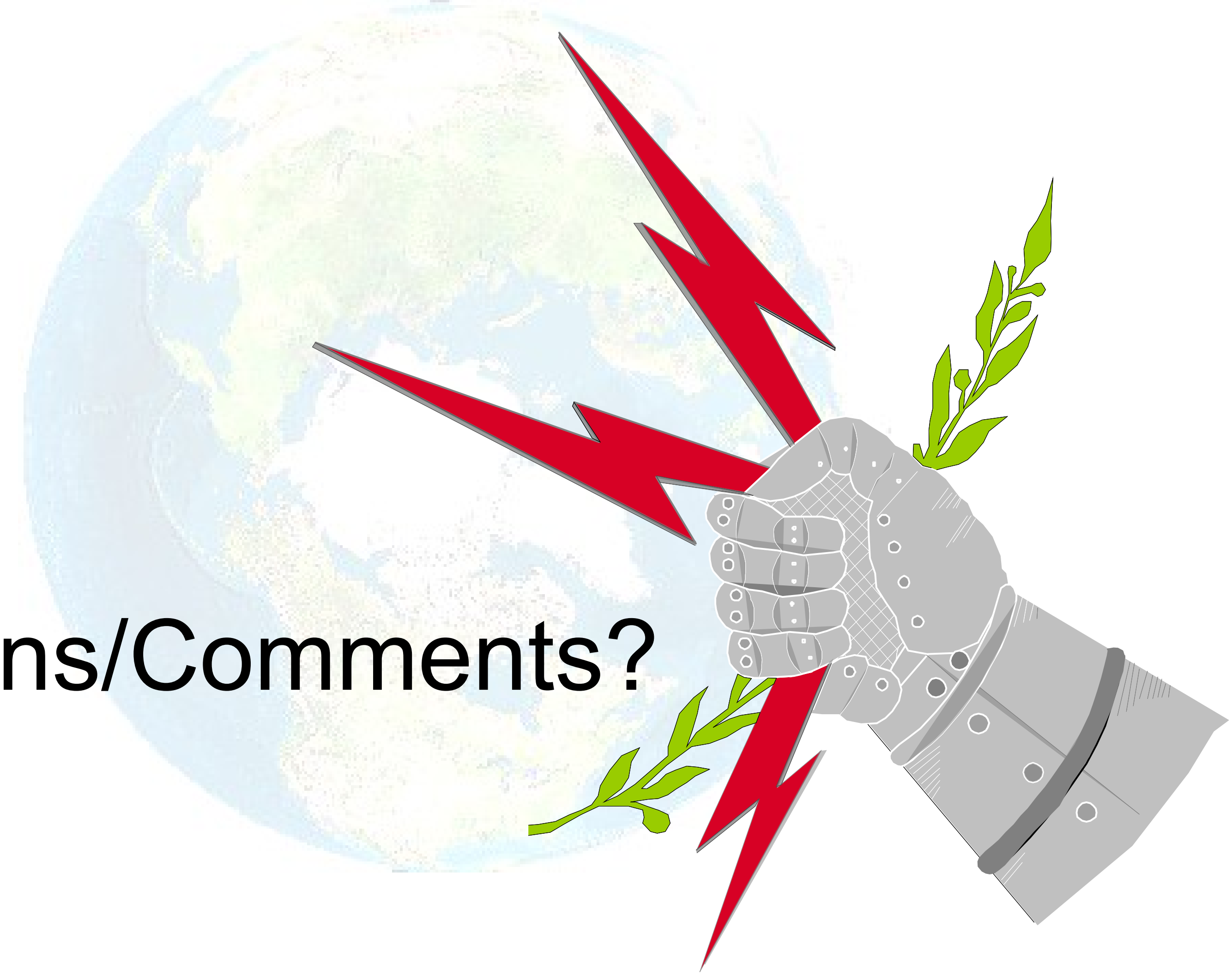
- **Information Sharing is Key to Decision Making**
- **Enabled Through STRATCOM'S Strategic Knowledge Integration Web (SKI Web) Portal**
  - Every Soldier, Sailor, Airman, and Marine in STRATCOM – around the globe – can share information with our 4-star commander on a 24/7 basis…and vice versa!
  - A never-ending ops-intel meeting
  - Everyone can participate by blogging



"It's more important to have some less-than-perfect information than no information at all…or perfect information late." ***General Cartwright***

Summary

- The nature of networks means no system is an island, so we must continue those partnerships we have forged with federal government, local government, industry, and academia to share information and experiences -- in near real time and in forums such as this -- in order to effectively combat the threats in cyberspace.



Questions/Comments?