DON Cybersecurity/Information Assurance Workforce Management

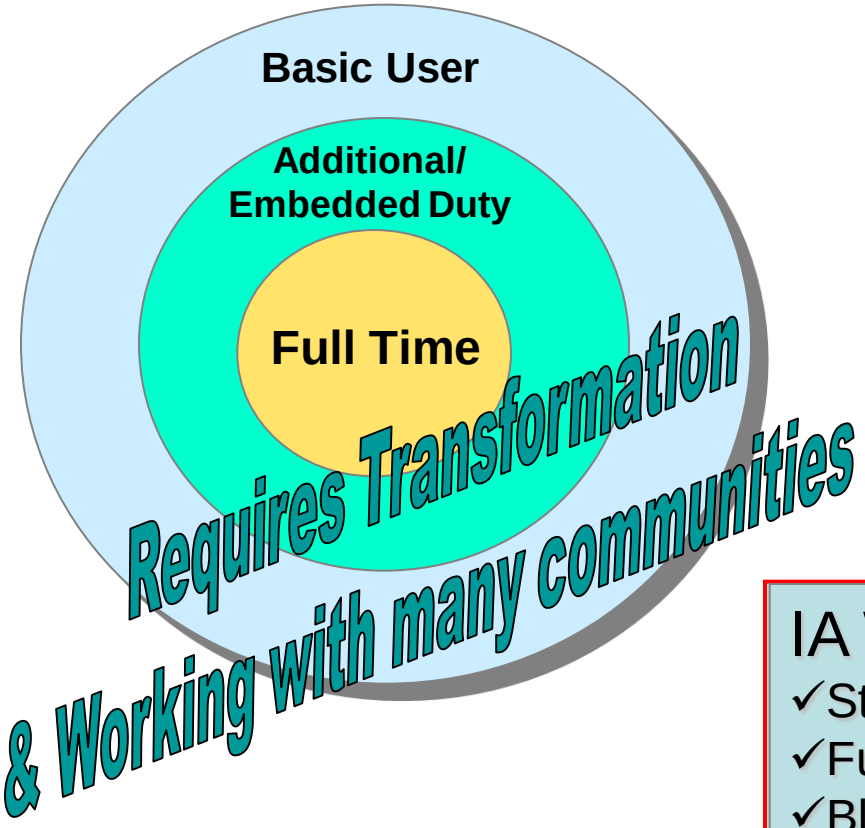
Chris Kelsall
DON CIO,
Director, Cyber/IT Workforce

23 March 2010

Steps to Transform IAWF Management

- Charter DON team to determine best approach
- Establish governance due to complexity - Cybersecurity/IAWF
- Establish common lexicon
- Write policy
  - Establish DON standards and consistency
  - Define Metrics
  - Develop Compliance reporting and feedback loop
- Develop Communications Plan (conferences, articles, memos)
- Promulgate Implementation Plan
- Provide annual direction from DON CIO
- Provide direction from Service operational/tactical leadership
- Share best practices and “lessons learned”
- Reinforce enterprise requirements

Defining the Enterprise IAWF



IA Professional

- Civilian
- Contractor
- Officer & Enlisted
- Active & Reserve
- Ashore & Afloat

IA Workforce Transition to:

✓Standardized DON workforce
✓Full Time Professionals
✓Blended Training Solution
✓NIST/CNSS Standards
✓Certified
✓Electronically Managed

2005-2008 IA Workforce Working Group Construct

Enterprise-wide Common Approach
(Reduce Redundant Efforts/Leverage Best Practices)

Manpower and Personnel

-IA Data Call
-IA Competency Management
-IA Workforce Management Policy

Membership:
TYCOMS
Operations Functionals
Technical Experts
Human Resources

OPR: DON CIO
OCR: HQMC/OPNAV N61/NNWC

Training and Certification

-Training Path Standard
-Certification Process
-Implementation Plans
-XML/SCORM e-learning Schema

Membership:
Training Representatives
Technical Experts
TYCOMS
Fleet/Operating Forces

OPR: MPT&E/TECOM
OCR: HQMC/CNO N61/NNWC

Workforce Management e-Solution

-Requirements Document
-DoD Visibility (DMDC, DCPDS, CVS)
-Funding
-User Friendly paperless test processes

Membership:
Manpower, Personnel, Training, Human Resources

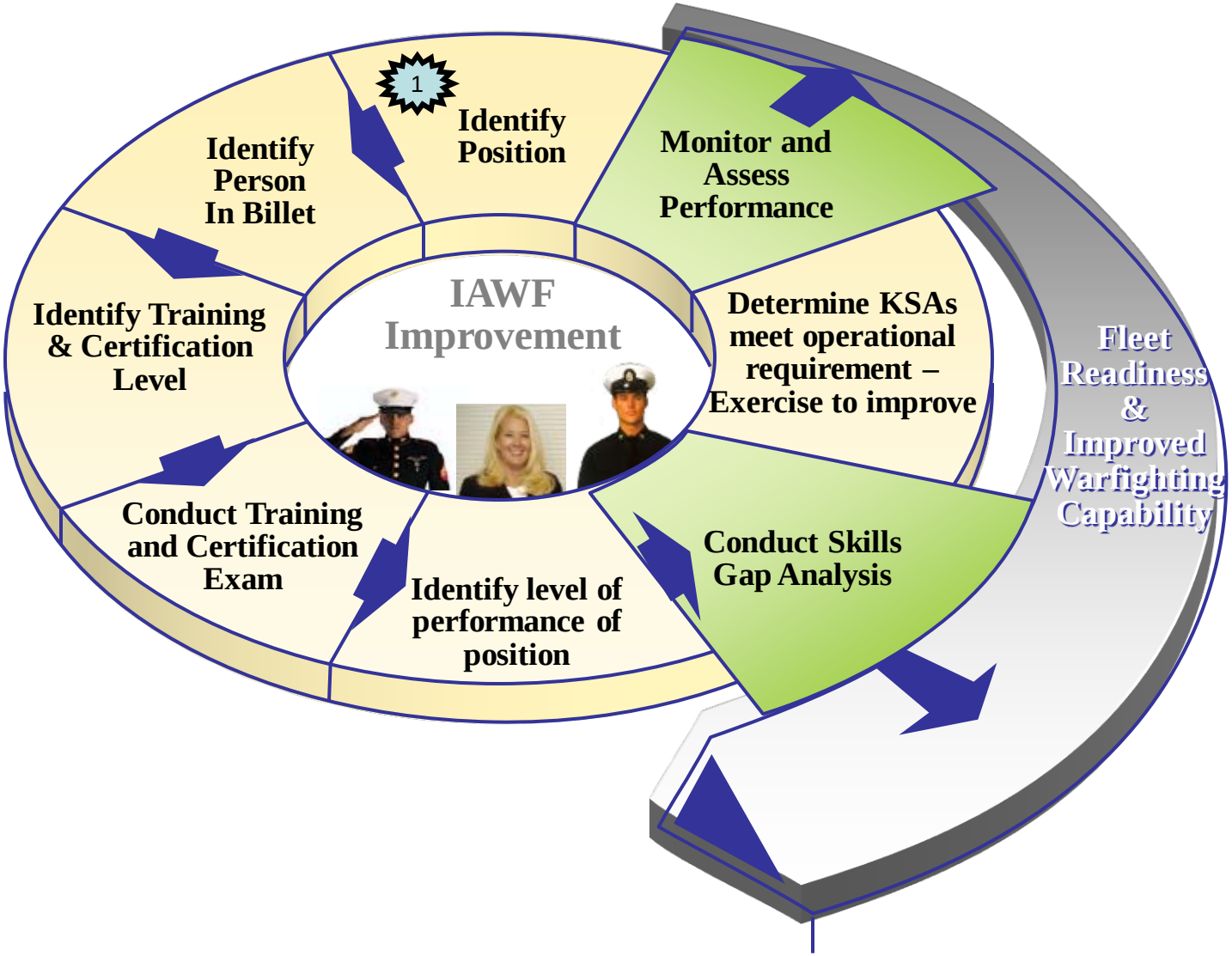
OPR: MPT&E/TECOM
OCR: HQMC/CNO N61/NNWC

CND SP Committee
IASAE Committee

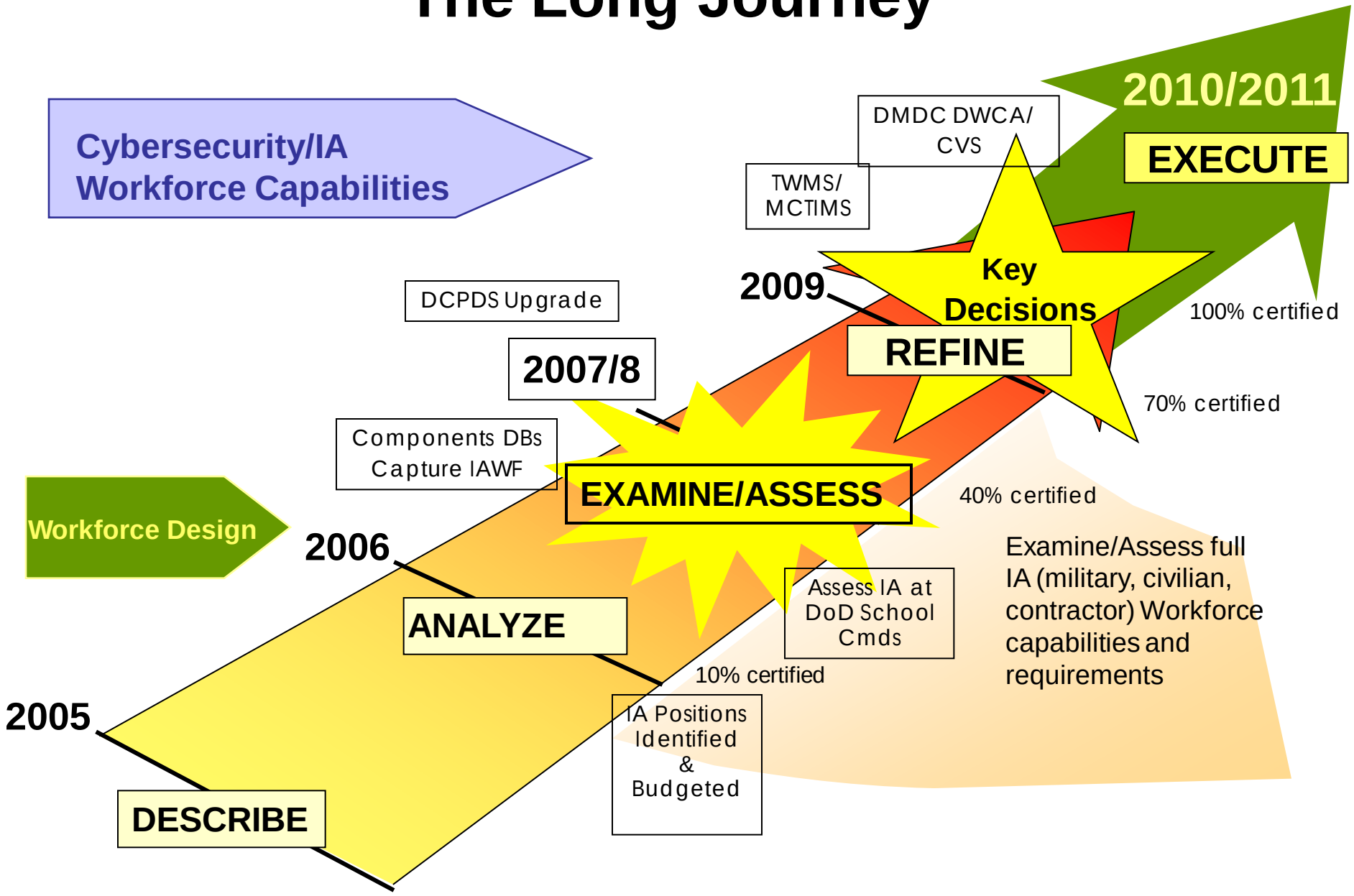
Membership:
Communities of Interest

Simultaneous Development and Integration

Meeting Operational Requirements



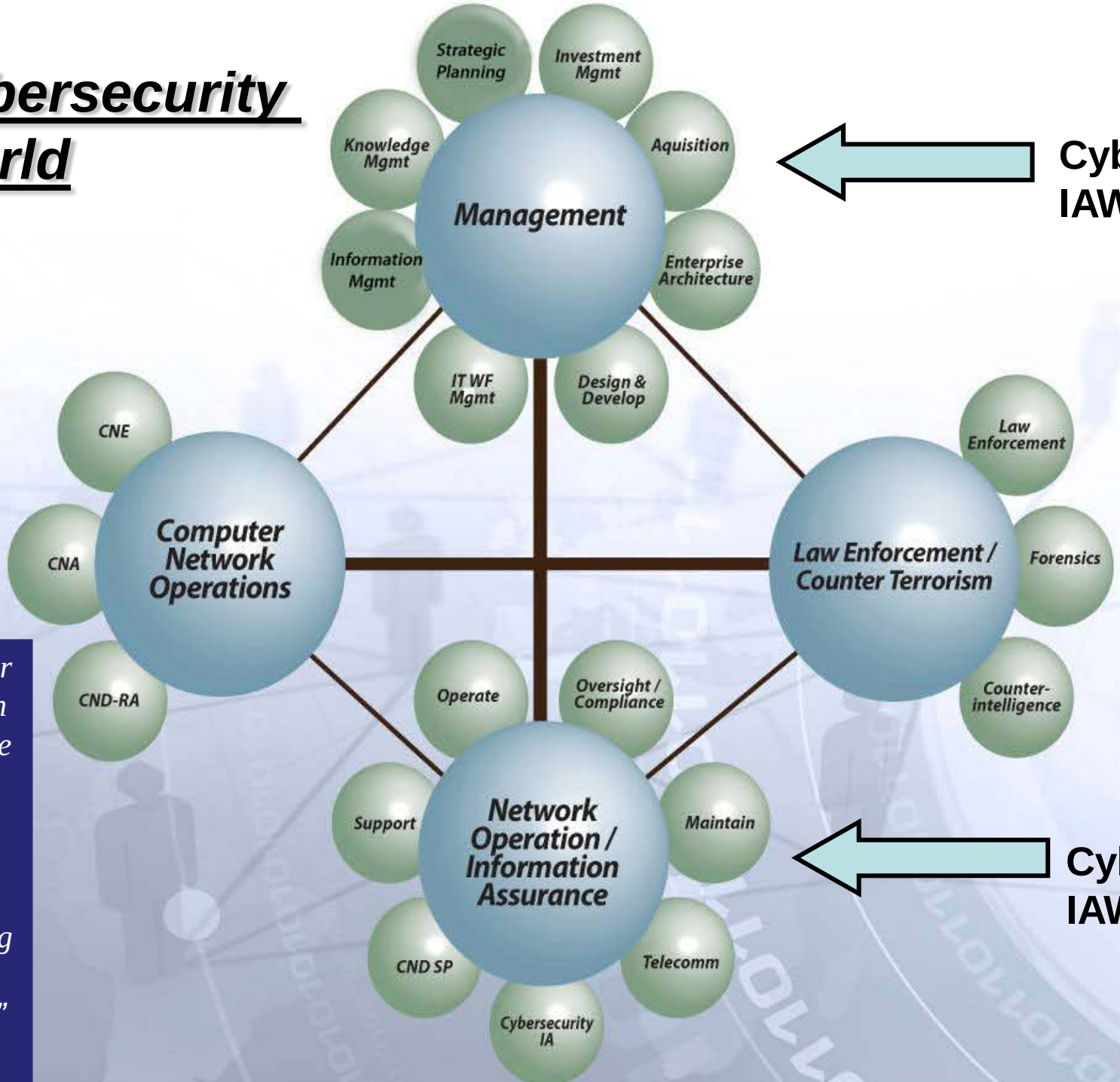
The Long Journey



The Future

- New Certifications
  - Cyber Attack/Exploit
  - Law Enforcement
  - Counterintelligence
- Currency
  - Continuing Education
  - Exercises/Simulations
  - Rapid Education and Training Deployment
- Educators and Trainers
  - Qualified and Current
  - Established Career Path
  - Community Information Sharing

Cybersecurity World



Cybersecurity/ IAWF

Cybersecurity/ IAWF

*nnect our
the men
tip of the
hey are
yer or
orward
n Iraq.
ust bring
nse of
t we do."*

N CIO

Questions

Chris Kelsall
DON CIO,
Director, Cyber/IT Workforce
chris.t.kelsall@navy.mil
www.doncio.navy.mil

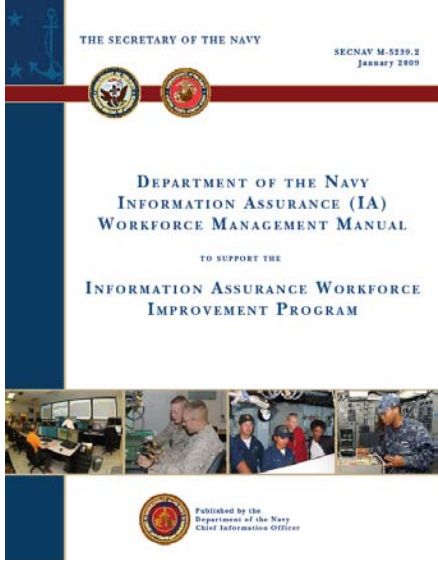
23 March 2010

Oversight and Compliance

IAWF MOCC (Chartered 16 March 2009)

- MOCC Executive Committee (DON CIO, DDCIO Navy and Marine Corps Designees) will:
  - Report to the DON Information Executive Committee (IEC)
  - Continue to make recommendations to OSD DIAP regarding the IA WIP
  - Provide DON Requirements to the Commercial Vendors
  - Communicate compliance requirements
  - Make IA WIP command assist visits
  - Monitor command commercial certification status to ensure compliance
  - Support Cybersecurity (IA) workforce roles development

Direction – Commands are required to: identify IA billets and people; train and certify; and electronically track



- Federal Information Security Management Act
- DODD 8570.01 Information Assurance Training, Certification, and Workforce Management
- DOD 8570.01- M Information Assurance Workforce Improvement Program
- SECNAVINST M-5239.3B DON Information Assurance Program
- SECNAVMAN 5239.2 IAWF Management Manual to Support IA WIP
- Management Oversight and Compliance Council (IAWF MOCC) Charter of 16 March 2009.
- DON CIO 021504Z FEB 10 MSG, Subj: Cybersecurity/IA Workforce Improvement Program Implementation Status/CY 2010 Action Plan
- SECNAVINST 5239.x: IA Workforce Management Oversight and Compliance (draft - in flag level chop)

Ongoing initiatives which will affect our Future Cybersecurity/IA Workforce Construct

- **Comprehensive National Cybersecurity Initiative** (CNCI) to secure government networks, protect against constant intrusion attempts, and anticipate future threats.
- **DoD and DON Cyber/IM/IT) Strategic Plans** for achieving information advantage.
- **National Military Strategy for Cyberspace Operations** (NMS-CO), **Network Operations** (NetOps) construct for operating and defending the Global Information Grid (GIG). Under United States Strategic Command (USSTRATCOM), - NetOps with other cyber operations - a Sub-unified **US Cyber Command** with subordinate **FLTCYBERCOM and MARCYBERCOM** structure.
- **IA Component of the GIG** integrated Architecture and strategies and programs for delivering key identity and IA capabilities as enterprise services.