THE SECRETARY OF THE NAVY

SECNAV M-5000.2
DECEMBER 2008

DEPARTMENT OF THE NAVY

ACQUISITION AND CAPABILITIES GUIDEBOOK

PUBLISHED BY
THE DEPUTY ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)
ACQUISITION AND LOGISTICS MANAGEMENT

DEPARTMENT OF THE NAVY
OFFICE OF THE ASSISTANT SECRETARY
RESEARCH, DEVELOPMENT AND ACQUISITION
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

December 22, 2008

FOREWORD

This Department of the Navy (DON) Acquisition and Capabilities Guidebook can be accessed through the following websites: the Department of the Navy Issuances Web site http://doni.daps.dla.mil/ under Manuals, the DON Research, Development and Acquisition Web site http://acquisition.navy.mil/ under "Policy and Guidance" and the Defense Acquisition University website https://akss.dau.mil/default.aspx under "AT&L Knowledge Sharing System (AKSS)," under "AKSS Menu," under "Policy Documents," under "Organizations," under "Navy/Marine Corps Common," under "Document Type: Discretionary," as "DON Acquisition and Capabilities Guidebook." This Guidebook is structured after the chapter/enclosure/paragraph numbering sequence of SECNAVINST 5000.2D. Major paragraph titles or headings from SECNAVINST 5000.2D are cited in this Guidebook for continuity and even for cases where no additional discretionary guidance is provided. The enclosures in this Guidebook include paragraphs for discretionary guidance other than those paragraphs included from SECNAVINST 5000.2D that are mandatory policy. This Guidebook is intended to be used as a companion document to SECNAVINST 5000.2D. This Guidebook contains citations from SECNAVINST 5000.2D and other mandatory references for process clarification. While the Guidebook does not introduce new or additional mandatory policy, the dynamic nature of the Capabilities Development Process demands continuous communication between all participants. As the Capabilities Development and Acquisition Management Processes mature, policy changes may affect acquisition strategies and timelines. Timely assessment of the change, coupled with the appropriate acquisition strategy adjustment, may be vital to the preservation of an acquisition timeline. While this guidebook references DoDI 5000.02 of 8 Dec 08 and some of its paragraphs, the acquisition decision point and phase names of DoDI 5000.2 of 12 May 03 have been retained to be consistent with SECNAVINST 5000.2D, but will be updated in the next version of SECNAVINST 5000.2 and its companion guidebook.

Enclosure (1) is a Table of Contents for the Guidebook. Enclosures (2) through (9) are respectively Chapters 2 through 9. Selected paragraphs from SECNAVINST 5000.2D shown in brackets [in **bold *italics***] are mandatory policy. Other paragraphs provide discretionary guidance as indicated by the verbs "should" or "may." Paragraphs from enclosures (3) and (5) of SECNAVINST

5000.2D are included in this Guidebook for more complete coverage of acquisition strategy and test and evaluation, respectively. Future releases of the Guidebook may contain more or less discretionary guidance as appropriate.

Enclosure (10) is a historical list of instructions, orders, and memoranda cancellations that occurred when SECNAVINST 5000.2B was issued. Enclosure (11) is a Glossary. Enclosure (12) is an Acronym List. Additional enclosures will be added as the need arises.

The enclosures of the Guidebook are:

Encl: (1) Chapter 1 Table of Contents
(2) Chapter 2 Capabilities Development and Acquisition Management Processes
(3) Chapter 3 Statutory, Regulatory, and Contract Reporting Information and Milestone Requirements
(4) Chapter 4 Information Technology (IT) Considerations
(5) Chapter 5 Integrated Test and Evaluation
(6) Chapter 6 Resource Estimation
(7) Chapter 7 Systems Engineering and Human Systems Integration
(8) Chapter 8 Acquisition of Services
(9) Chapter 9 Program Management
(10) Chapter 10 SECNAVINST, OPNAVINST, and Marine Corps Orders Cancellations (prior SECNAVINST 5000.2C cancellations retained for historical purposes)
(11) Chapter 11 Glossary
(12) Chapter 12 List of Acronyms

Seán F. Crean
Rear Admiral, SC, U.S. Navy
Deputy Assistant Secretary of the Navy
(Acquisition and Logistics Management)

Distribution:
Electronic only, via Department of the Navy (DON) Issuances Web site http://doni.daps.dla.mil/, DON Research, Development and Acquisition Web site http://acquisition.navy.mil/ and Defense Acquisition University AT&L Knowledge Sharing System (AKSS) Web site https://akss.dau.mil/default.aspx

Chapter 1
Table of Contents

Chapter 2 Capabilities Development and Acquisition Management Processes
2.1 Capabilities Development Process
2.1.1 DON Principal Capabilities Points of Contact
2.1.1.1 Chief of Naval Operations (CNO)/Commandant of the Marine Corps (CMC) Responsibilities
2.1.1.2 Navy Program and Resource Sponsor Responsibilities
2.1.1.3 Deputy CNO (Integration of Capabilities and Resources) (CNO (N8)) Responsibilities
2.1.1.4 Deputy CNO (Communication Networks) (CNO (N6)) Responsibilities
2.1.2 DON Capabilities Development and Processing Procedures
2.1.2.1 Naval Capabilities Development Process
2.1.2.2 Marine Corps Capabilities Development Process for Programs with Navy Fiscal Sponsorship
2.1.2.3 Weapon and Information Technology Systems Capabilities Development and Processing Procedures
2.1.2.3.1 Initial Capabilities Documents (ICDs)
2.1.2.3.2 Capability Development/Production Documents (CDD/CPDs)
2.1.2.3.3 ICD/CDD/CPD Formulation
2.1.2.3.4 Navy Capabilities Document Flow Process
2.1.2.3.4.1 Roles and Responsibilities
2.1.2.3.4.2 Joint Capabilities Integration and Development System (JCIDS) Document Routing and Review Process
2.1.2.3.5 Navy Capabilities Document Change Process
2.1.2.3.5.1 Changes to Key Performance Parameter (KPP) Requirements
2.1.2.3.5.2 Changes to Key System Attributes (KSAs)
2.1.2.3.5.3 Changes to Non-Key Performance Parameters (Non-KPPs) or Non-Key System Attributes (Non-KSAs)
2.1.2.3.5.4 Administrative Changes
2.1.2.3.5.5 Staffing and Approval Matrix for Changes to Capability Documents
2.1.2.4 Fleet Modernization Program
2.1.2.5 FORCEnet
2.1.2.5.1 FORCEnet Requirements/Capabilities and Compliance Process
2.1.2.5.2 Support to Naval Capabilities Development Process
2.1.2.5.3 FORCEnet Consolidated Compliance Checklist
2.1.2.5.4 FORCEnet Compliance Governance Process
2.1.2.5.5 Roles and Responsibilities
2.2 Acquisition Management Process
2.3 Overview of the Acquisition Management Process
2.3.1 Integrated Product Teams (IPTs)
2.3.1.1 Overarching Integrated Product Teams (OIPTs)
2.3.1.2 Working Integrated Product Teams (WIPTs)
2.3.2 Acquisition Coordination Teams (ACTs)
2.4 Categories of Acquisition Programs and Milestone Decision Authorities

2.5 Capability Concept Development and Program Decision Points and Phases
2.5.1 User Needs and Technology Opportunities
2.5.2 Program Tailoring
2.5.3 Program Decision Points Tailoring
2.5.4 Program Decision Points and Phases
2.5.4.1 Concept Decision
2.5.4.2 Concept Refinement
2.5.4.3 Milestone A
2.5.4.4 Technology Development
2.5.4.5 Milestone B
2.5.4.6 System Development and Demonstration
2.5.4.6.1 System Integration
2.5.4.6.2 Design Readiness Review
2.5.4.6.3 System Demonstration
2.5.4.7 Milestone C
2.5.4.8 Production and Deployment
2.5.4.9 Operations and Support
2.5.4.9.1 Sustainment
2.5.4.9.2 Disposal
2.5.5 Modifications
2.6 Review of the Legality of Weapons Under International Law and Compliance with Arms Control Agreements
2.7 Non-Acquisition Programs
2.7.1 Management of Non-Acquisition Programs
2.8 Rapid Deployment Capability (RDC) Process and Procedures
2.9 Executive Review Procedures
2.9.1 DON Program Decision Process
2.9.2 Information Technology (IT) Acquisition Board (ITAB) Reviews
2.9.3 Defense Space Acquisition Board (DSAB) Reviews
2.9.4 Defense Business System Management Committee (DBSMC) Certification and Approval
2.9.4.1 Defense Business System Definition
2.9.4.2 Roles and Responsibilities
2.10 Source Selection Authority (SSA)
2.10.1 ACAT I, IA, and II Programs
2.10.2 ACAT III, IV, and Abbreviated Acquisition Programs
2.10.3 Other Competitively Negotiated Acquisitions
2.10.4 Source Selection Advisory Council (SSAC)
2.10.5 Source Selection Evaluation Board (SSEB)
2.10.6 ASN(RD&A) Source Selection Briefing
2.11 Two-Pass/Six-Gate DON Requirements and Acquisition Governance Process
2.11.1 Purpose
2.11.2 Objective
2.11.3 Scope and Applicability
2.11.4 Organization and Procedures
2.11.4.1 Concept Decision and Concept Refinement Phase
2.11.4.1.1 Pass 1
2.11.4.1.1.1 Gate 1
2.11.4.1.1.2 Gate 2
2.11.4.1.1.3 Gate 3
2.11.4.2 Milestone A and Technology Development Phase
2.11.4.2.1 Pass 2

2.11.4.2.1.1 Gate 4
2.11.4.3 Milestone B and System Development and Demonstration Phase
2.11.4.3.1 Pass 2
2.11.4.3.1.1 Gate 5
2.11.4.3.1.2 Gate 6
2.11.4.4 DON Requirements/Acquisition Gate Review Membership
2.11.4.4.1 Chairperson
2.11.4.4.2 Principal Members
2.11.4.4.3 Advisory Members
2.11.4.5 DON Requirements/Acquisition Individual Gate Membership and Input/Exit Criteria
2.11.4.6 System Design Specification (SDS) Description
2.11.5 Responsibilities
2.11.5.1 ASN(RD&A)
2.11.5.2 CNO/CMC
2.11.5.3 DCNO (N8)/DC, CD&I
2.11.5.4 PEOs/SYSCOMs
2.11.5.5 ASN(FM&C)FMB
2.11.5.6 OGC
2.11.6 Industry Involvement
Annex 2-A Navy Requirement/Capability Documents Flow
Annex 2-B Initial Capabilities/Capability Development/ Production Document Signature Page
Annex 2-C Initial Capabilities Document (ICD) Content Guidance
Annex 2-D Capability Development/Production Document (CDD/CPD) Content Guidance
Annex 2-E FORCEnet Consolidated Compliance Checklist for Development of IT, including National Security Systems (NSS), JCIDS Capabilities Documents and Acquisition Implementation
Annex 2-F Weapon System and IT System Programs ACAT Designation/Change Request (Content)

Chapter 3 Statutory, Regulatory, and Contract Reporting Information and Milestone Requirements
3.1 Program Information
3.2 Exit Criteria
3.3 Technology Maturity
3.4 Technology Development and Acquisition Strategies
3.4.1 General Considerations for a Technology Development Strategy and an Acquisition Strategy
3.4.2 Requirements/Capability Needs
3.4.3 Program Structure
3.4.4 Risk
3.4.4.1 Interoperability and Integration Risk
3.4.5 Program Management
3.4.5.1 Integrated Digital Environment (IDE)
3.4.5.2 Technical Representatives at Contractor Facilities
3.4.5.3 Government Property in the Possession of Contractors (GPPC)

3.4.5.4 Planning for Simulation-Based Acquisition (SBA) and Modeling and Simulation (M&S)
3.4.6 Design Considerations Affecting the Acquisition Strategy
3.4.6.1 Open Architecture
3.4.6.2 Interoperability and Integration
3.4.6.2.1 Integrated Architecture
3.4.6.3 Aviation Critical Safety Items
3.4.6.4 Information Assurance
3.4.6.5 Standardization and Commonality
3.4.6.6 Protection of Critical Program Information and Anti-Tamper (AT) Measures
3.4.7 Support Strategy
3.4.7.1 Human Systems Integration (HSI)
3.4.7.2 Environmental, Safety, and Occupational Health (ESOH) Considerations
3.4.7.3 Demilitarization and Disposal Planning
3.4.7.4 Post Deployment Performance Review
3.4.7.5 Program Protection Planning
3.4.7.6 Product Support
3.4.7.6.1 Product Support Management Planning
3.4.7.7 Planning for Parts and Materials Obsolescence
3.4.8 Business Strategy
3.4.8.1 International Cooperation
3.4.8.1.1 International Cooperative Strategy
3.4.8.1.2 International Interoperability
3.4.8.2 Competition
3.4.8.3 Warranties
3.5 Intelligence Support
3.6 Command, Control, Communications, Computers, and Intelligence (C4I)/Information Support
3.7 Electromagnetic Environmental Effects (E3) and Electromagnetic Spectrum Certification and Supportability
3.7.1 Electromagnetic Environmental Effects (E3)
3.7.2 Electromagnetic Spectrum Certification and Supportability
3.7.2.1 Electromagnetic Spectrum Certification Compliance
3.7.2.2 Electromagnetic Spectrum Supportability
3.8 Technology Protection
3.8.1 Anti-Tamper Measures
3.8.1.1 Program Protection Plan AT Annex
3.9 Periodic Reporting
3.9.1 Program Plans
3.9.2 Acquisition Program Baseline (APB) Reporting
3.9.3 Defense Acquisition Executive Summary (DAES)
3.9.3.1 DAES Reporting
3.9.4 Selected Acquisition Report (SAR)
3.9.5 Unit Cost Reports (UCRs)
3.9.6 Past Performance Reporting/Reports
3.9.7 Consolidated Acquisition Reporting System (CARS)
3.10 Program Certification and Assessments
3.10.1 Certification Requirements at Milestone A
3.10.2 Certification Requirements at Milestone B

3.10.3 Assessments Required Prior to Approving the Start of Construction on First Ship of Shipbuilding Program
Annex 3-A Weapon System and IT System Programs Acquisition Program Baselines (APBs)/APB Deviations

Chapter 4 Information Technology (IT) Considerations
4.1 Clinger-Cohen Act (CCA) (40 U.S.C., Subtitle III) Compliance
4.1.1 CCA Compliance Package Development and Processing for ACAT IAM, IAC, ID, IC, and II Programs containing Mission-Critical (MC) or Mission-Essential (ME) IT Systems including National Security Systems (NSS)
4.1.2 CCA Compliance Package Development and Processing for ACAT III, IV, and Abbreviated Acquisition Program (AAP) Programs containing MC or ME IT Systems including NSS
4.2 Contracts for Acquisition of MC or ME IT Systems including NSS
4.3 Information Integration and Interoperability
4.4 Information Assurance (IA) Program Manager (PM) Responsibilities
4.4.1 Information Assurance and Integrated Architectures
4.4.2 IA Strategy Content
4.4.2.1 Policies, Standards, and Architectures
4.4.2.1.1 Benchmark
4.4.2.1.2 Potential Sources
4.4.2.2 Certification and Accreditation
4.4.2.2.1 Benchmark
4.4.2.2.2 Potential Sources
4.4.3 IA Workforce
4.5 Records Management
4.6 Human Systems Integration and Environment, Safety, and Occupational Health (ESOH) Considerations

Chapter 5 Integrated Test and Evaluation
5.1 Integrated Test and Evaluation (T&E) Overview
5.2 DON Points of Contact and Responsibilities for T&E
5.2.1 Principal Navy Points of Contact and Responsibilities
5.2.1.1 Chief of Naval Operations (CNO) (N091) Director, Test and Evaluation and Technology Requirements
5.2.1.2 Program Manager (PM)
5.2.1.2.1 Personnel Security Clearances
5.2.1.3 Commander, Operational Test and Evaluation Force (COMOPTEVFOR)
5.2.1.4 Naval Systems Commands (SYSCOMs)
5.2.1.4.1 Naval Air Systems Command (NAVAIRSYSCOM)
5.2.1.4.1.1 Naval Air Systems Command Technical Assurance Board (NTAB)
5.2.1.4.2 Weapons System Explosive Safety Review Board (WSESRB)
5.2.1.4.3 Space and Naval Warfare Systems Command (SPAWAR) Office of the Chief Engineer (CHENG)
5.2.1.5 Office of Naval Intelligence (ONI)
5.2.2 Principal Marine Corps Points of Contact and Responsibilities
5.2.2.1 Deputy Commandant for Manpower and Reserve Affairs

(DC,M&RA)
5.2.2.2 Deputy Commandant for Installations and Logistics (DC,I&L)
5.2.2.3 Director, Marine Corps Intelligence Activity (MCIA)
5.2.2.4 Deputy Commandant, Combat Development and Integration (DC,CD&I)
5.2.2.5 Commanding General, Marine Corps Systems Command (CG, MARCORSYSCOM)
5.2.2.6 Director, Marine Corps Operational Test and Evaluation Activity (MCOTEA)
5.2.2.7 Marine Forces
5.2.3 Acquisition Items Exempt from T&E Provisions within SECNAVINST 5000.2D
5.2.3.1 Items Exempt
5.2.3.2 T&E Considerations that Apply to Exempt Items
5.3 T&E Strategy
5.3.1 Preparation and Milestones
5.3.2 Strategy Approval
5.4 T&E Planning
5.4.1 Early Planning for Integrated T&E
5.4.2 Testing Increments in Evolutionary Acquisition
5.4.2.1 Innovative Testing
5.4.2.2 Initial Operational Test and Evaluation (IOT&E)
5.4.2.3 Software Intensive Systems
5.4.2.4 T&E of Ships
5.4.2.4.1 Ship Programs without New Development
5.4.2.5 T&E of Space Systems
5.4.3 Test and Evaluation Working Integrated Product Team (T&E WIPT)
5.4.4 Navy Test and Evaluation Coordination Group (TECG)
5.4.4.1 TECG Membership
5.4.4.2 Distribution of TECG Results
5.4.4.3 TECG for a Consolidated Cryptologic Program (CCP)
5.4.5 T&E Funding Responsibility
5.4.5.1 Developing Activity Responsibilities
5.4.5.2 Fleet Commanders Responsibilities
5.4.5.3 Board of Inspection and Survey (INSURV) Responsibilities
5.4.5.4 Non-Acquisition Programs Responsibilities
5.4.6 Research, Development, Test and Evaluation (RDT&E) Support Provided by Fleet Commanders
5.4.6.1 Scheduling RDT&E Fleet Support
5.4.6.1.1 Requests
5.4.6.1.2 Fleet Support Priorities
5.4.6.2 Unscheduled RDT&E Support Requirements
5.4.6.3 RDT&E Fleet-Support Scheduling Agent
5.4.6.4 Conduct of At-Sea T&E
5.4.7 Test and Evaluation Master Plan (TEMP)
5.4.7.1 Milestone B TEMP Approval for IT Systems, including NSS, and Spectrum Dependent Systems

5.4.7.2 Milestone C TEMP Approval for IT Systems, including NSS, and Spectrum Dependent Systems
5.4.7.3 Capabilities and Key Performance Parameter (KPP) Traceability to Critical Operational Issues (COI)
5.4.7.4 Performance Thresholds and Critical Technical Parameters (CTPs)
5.4.7.5 Test Planning for Commercial and Non-Developmental Items
5.4.7.6 Use of Existing T&E Infrastructure
5.4.7.7 Environmental Protection
5.4.7.7.1 Environmental, Safety and Occupational Health (ESOH)
5.4.7.7.2 Responsibilities for Environmental Compliance During Testing
5.4.7.7.3 Safety Releases for Testing
5.4.7.8 Operational Test and Evaluation (OT&E) for Non-Acquisition Programs
5.4.7.9 Modeling and Simulation (M&S)
5.4.7.10 Interoperability Testing and Certification
5.4.7.10.1 Joint Interoperability Process and Support
5.4.7.10.1.1 Three Types of Joint Interoperability Test Command (JITC) Certification Reports
5.4.7.11 Information Assurance (IA) and Information Systems Security Certification and Accreditation
5.4.7.12 Anti-Tamper Verification and Validation Testing
5.4.7.13 Test and Evaluation Identification Number (TEIN) Assignment
5.4.7.13.1 Pre-requisite Documentation
5.4.7.13.2 Program Groups
5.4.7.13.3 Consolidated Cryptologic Programs (CCP)
5.4.7.13.4 Inactive TEINs
5.4.7.14 TEMP Approval
5.4.7.14.1 TEMP Timing
5.4.7.14.2 TEMP Drafting/Submitting
5.4.7.15 TEMP Distribution
5.4.7.16 TEMP Updates
5.4.7.16.1 TEMP Revision
5.4.7.17 Administrative Change to TEMP
5.4.7.17.1 Determination on Administrative Change to a TEMP
5.4.7.17.2 Procedure for an Administrative Change to a TEMP
5.5 Developmental Test and Evaluation (DT&E)
5.5.1 DT&E Data
5.5.2 Information Assurance and Security Certification during Developmental Test (DT)
5.5.3 Production Qualification Test and Evaluation
5.5.4 DT&E Phases and Procedures
5.5.4.1 DT-A
5.5.4.2 DT-B/DT-C (TECHEVAL)
5.5.4.3 DT-D
5.5.4.4 DT&E Schedules
5.5.4.5 Operator and Maintenance Training
5.5.4.6 Live Fire Test and Evaluation (LFT&E)*
5.5.4.7 United States Marine Corps (USMC) Developmental Test and Evaluation
5.5.4.7.1 DT&E of Amphibious Vehicles

5.6 Certification of Readiness for Operational Testing
5.6.1 DON Criteria for Certification
5.6.2 Navy Procedures for Certification
5.6.2.1 Certification for OT Without T&E Exceptions
5.6.2.2 Certification for OT With T&E Exceptions
5.6.3 Marine Corps Procedures for Certification
5.6.4 Navy T&E Exceptions
5.6.4.1 Waivers
5.6.4.2 Deferrals
5.6.4.2.1 When Deferrals are Appropriate
5.6.4.2.2 Limitations to Test
5.6.4.2.3 Resolutions of COIs
5.6.4.3 CNO (N091) Approval of a Deferral Request
5.6.5 Navy Waiver and Deferral Requests
5.6.6 Marine Corps Waivers
5.7 Operational Test and Evaluation (OT&E)
5.7.1 Independent OT&E
5.7.1.1 Navy Start of OT&E
5.7.1.2 Navy De-certification and Re-certification for OT&E
5.7.2 OT&E Plans
5.7.2.1 OT&E Phases and Procedures
5.7.2.1.1 Operational Assessments (OAs)
5.7.2.1.2 OT-A (EOAs)
5.7.2.1.3 OT-B (OA)
5.7.2.1.3.1 DT Assist
5.7.2.1.4 OT-C (IOT&E)/(Navy OPEVAL)
5.7.2.1.5 Combined DT/OT
5.7.2.1.6 Follow-on Operational Test and Evaluation (FOT&E)
5.7.2.1.6.1 OT-D
5.7.2.1.6.2 OT-E
5.7.2.1.6.3 Verification of Corrected Deficiencies (VCD) for Navy Programs
5.7.2.1.7 OT Resource Requirements
5.7.2.2 OT of Computer Software
5.7.2.2.1 Baseline or Core Increment Testing
5.7.2.2.1.1 Mission Criticality/Software Risk Based Operational Testing
5.7.2.2.2 Revision or post Core Increment Testing
5.7.2.2.3 Use of Non-Operational Facilities
5.7.2.2.4 Use of Modeling, Simulation, and Signal Stimulation in Software Testing
5.7.2.2.5 Use of Non-Operational Test Agency (OTA) Testers to Conduct OT&E
5.7.2.2.6 Role of the Developing Activity (DA) and the OTA in OT&E of Software
5.7.2.2.7 Designation of Software Testing and Software Qualification Testing (SQT)
5.7.2.2.8 Software Operational Testing and Interoperability, Security, or Information Assurance Certification
5.7.2.2.9 Changes to Software Operational Requirements
5.7.2.2.9.1 Statement of Functionality (SOF)
5.7.2.2.10 System of Systems Testing
5.7.2.2.11 Resolution of Disputes Involving Operational Testing of Software

5.7.3 Operational Test (OT) for Configuration Changes
5.7.4 OT for Information Assurance and System Security Certification and Accreditation
5.7.5 Quick Reaction Assessment (QRA)
5.7.6 OT&E Information Promulgation
5.7.6.1 MDA Briefing
5.7.6.2 OT Data Release
5.7.7 Use of Contractors in Support of OT&E
5.7.8 Visitors
5.7.9 Special T&E Considerations
5.7.9.1 T&E of Modifications
5.7.9.2 T&E of Non-Developmental Items/Commercial Off-The-Shelf (NDI/COTS)
5.7.9.3 Extension of Application
5.8 Annual Office of the Secretary of Defense (OSD) T&E Oversight List
5.9 Live Fire Test and Evaluation (LFT&E)
5.9.1 LFT&E of Ships
5.10 Foreign Comparative Testing (FCT)
5.10.1 Programs Defined by Statute
5.10.2 Navy Management of Comparative Testing
5.10.3 Developing Activity_(DA) Comparative Testing Responsibilities
5.11 Test and Evaluation Reporting
5.11.1 DoD Component (DON) Reporting of Test Results
5.11.1.1 DT&E Reports
5.11.1.2 Navy OT&E Reports
5.11.1.2.1 Anomaly Reports
5.11.1.2.2 Deficiency Reports
5.11.1.3 Marine Corps Operational Test Reports (TRs)
5.11.1.4 OT&E Reporting Against the Threat of Record
5.11.2 LFT&E Report for Full-Rate Production Decision Review (FRP DR)
5.11.2.1 LFT&E Waivers
5.11.3 Beyond-Low Rate Initial Production Report
5.11.4 Director, Operational Test and Evaluation (DOT&E) Annual Report
5.11.5 Foreign Comparative Test Notification and Report to Congress
5.11.6 Electronic Warfare (EW) T&E Report
Annex 5-A Index of TES/TEMP Signature Page Formats
Annex 5-B Fleet RDT&E Support Request
Annex 5-C Test and Evaluation Identification Number Request Format
Annex 5-D Notional Schedule of Test Phases in the Acquisition Model
Annex 5-E Navy Certification of Readiness for OT Message Content
Annex 5-F Elements of Risk Assessment for Software Intensive System Increments
Annex 5-G Determining Appropriate OT&E for Software Intensive System Increments
Annex 5-H Software Intensive System Responsibilities for and Schedule of OT&E Actions

Chapter 6 Resource Estimation
6.1 Resource Estimates
6.1.1 Life-Cycle Cost Estimates
6.1.2 Cost Analysis Requirements Description (CARD)
6.1.3 Manpower Estimates
6.1.3.1 Manpower Considerations
6.2 Affordability
6.3 Contract Management Reports
6.3.1 Contractor Cost Data Reporting (CCDR) for Hardware and Software -– (DID DI-FNCL-81565B/81566B/81567B) and Software Resources Data Report (SRDR) –- (DID DI-MGMT-81739/81740)
6.3.2 Contract Performance Report (CPR) -- (DID DI-MGMT-81466A)
6.3.3 Integrated Master Schedule (IMS) -- (DID DI-MGMT-81650)
6.3.4 Contract Funds Status Report (CFSR) -– (DID DI-MGMT-81468)
6.4 Analysis of Alternatives (AoA)
6.4.1 Weapon System AoA
6.4.2 IT AoA
6.5 Cost as an Independent Variable (CAIV)
6.5.1 Cost/Schedule/Performance Tradeoffs
Annex 6-A Weapon System and IT System Programs Analysis of Alternatives Development Procedures

Chapter 7 Systems Engineering and Human Systems Integration
7.1 Systems Engineering
7.1.1 Manufacturing and Production
7.1.1.1 Test, Measurement, and Diagnostic System Support
7.1.1.1.1 Measurement Traceability and Compatibility
7.1.1.1.2 Measurement Technology
7.1.2 Quality
7.1.2.1 Past Performance
7.1.2.2 Deficiency Reporting
7.1.3 Acquisition Logistics and Sustainment
7.1.3.1 Life Cycle Logistics (LCL)
7.1.3.2 Total Life Cycle Systems Management (TLCSM)
7.1.3.3 Program Manager’s LCL Responsibility
7.1.3.4 Warfighter Supportability-Related Performance
7.1.3.5 Supportability
7.1.3.6 Supportability Analyses
7.1.3.7 Support Concepts
7.1.3.8 Support Data
7.1.3.8.1 Sources for Support Related Data
7.1.3.9 Support Resources
7.1.4 Open Architecture
7.1.5 Reliability, Availability, and Maintainability (RAM)
7.1.6 Interoperability and Integration
7.1.6.1 IT Design Considerations
7.1.6.2 DoD Architecture Framework/ Defense Information Technology Standards Registry (DISR)
7.1.6.2.1 Transformational Communications Architecture (TCA)
7.1.6.2.2 Joint Tactical Radio System (JTRS) Software Compliant Architecture (SCA)
7.1.6.2.3 Teleports

7.1.6.2.4 Joint Battle Management Command and Control (JMBC2)
7.1.6.3 FORCEnet Integrated Architecture
7.1.6.3.1 System of Systems (SoS) or Family of Systems (FoS) Integration and Interoperability Validation
7.1.6.3.2 FORCEnet Integrated Management Plan
7.1.6.3.3 FORCEnet Efficiency and Effectiveness
7.1.6.3.4 Roles and Responsibilities for FORCEnet Implementation Within the Acquisition Community
7.1.6.4 Interoperability and Integration Support
7.1.7 Survivability
7.1.8 Shipboard Systems Integration
7.1.9 Performance Specifications
7.1.9.1 System Performance for SoS and FoS Programs
7.1.9.2 Standardization and Commonality
7.1.10 Precise Time and Time Interval (PTTI) Support
7.1.11 Geospatial Information and Services (GI&S)
7.1.12 Natural Environmental Support
7.1.13 Electromagnetic Environmental Effects (E3) and Spectrum Supportability
7.1.14 Integrated Product and Process Development (IPPD)
7.1.14.1 Integrated Product Teams (IPTs) and IPPD
7.1.14.2 Integrated Technical Information Database
7.1.15 Modeling and Simulation (M&S)
7.1.16 Software Management
7.1.17 Commercial-Off-The-Shelf (COTS) Considerations
7.1.18 Metric System
7.1.19 Value Engineering (VE)
7.1.20 Accessibility Requirements
7.1.21 Government-Industry Data Exchange Program (GIDEP)
7.2 Human Systems Integration (HSI)
7.2.1 HSI in Acquisition
7.2.2 Manpower, Personnel, and Training (MPT)
7.2.2.1 Manpower and Personnel
7.2.2.2 Training
7.2.3 Human Factors Engineering (HFE)
7.2.4 Personnel Survivability
7.2.5 Habitability
7.3 Environmental, Safety, and Occupational Health (ESOH)
7.3.1 ESOH Compliance
7.3.2 National Environmental Policy Act (NEPA) and Executive Order (EO) 12114 Environmental Effects Abroad
7.3.3 Safety and Health
7.3.4 Hazardous Materials Management
7.3.5 Pollution Prevention
7.3.6 Explosives Safety
7.3.7 Aviation Critical Safety Items (CSIs)
7.3.8 Corrosion Prevention and Control
Annex 7-A Systems Engineering Plan (SEP) Signature Pages

Chapter 8 Acquisition of Services
8.1 Introduction
8.2 Applicability
8.3 Definitions
8.4 Responsibilities

8.5 Review and Approval Thresholds
8.6 Review Procedures
8.7 Outcomes
8.8 Metrics
8.9 Data Collection
8.10 Execution Reviews
8.11 Decision Authority Acquisition Management Responsibilities

Chapter 9 Program Management
9.1 Assignment of Program Executive Officer Responsibilities
9.2 International Cooperative Program Management
9.3 Joint Program Management

Chapter 10 SECNAVINST, OPNAVINST, and Marine Corps Orders Cancellations
Cancellations in SECNAVINST 5000.2C retained for historical purposes.

Chapter 11 Glossary

Chapter 12 List of Acronyms

Chapter 2
Capabilities Development and Acquisition Management Processes

References: (a) SECNAVINST 5000.2D
(b) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01F, Joint Capabilities Integration and Development System, of 1 May 07
(c) Chairman of the Joint Chiefs of Staff Instruction 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems, of 8 Mar 06
(d) Marine Corps Order (MCO) 3900.15B, Marine Corps Expeditionary Force Deployment System, of 10 Mar 08
(e) Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3170.01C, Operation of the Joint Capabilities Integration and Development System, of 1 May 07
(f) SECNAVINST 3501.1A
(g) DOD Instruction 5000.02, Operation of the Defense Acquisition System, of 8 Dec 08

2.1 Capabilities Development Process

[***fm SNI 5000.2D, 2.1: The Department of the Navy (DON) uses a capabilities-based approach to define, develop, and deliver technologically sound, sustainable, and affordable military capabilities. This approach is implemented via the Naval Capabilities Development Process (NCDP), the Expeditionary Force Development System (EFDS), and the Joint Capabilities Integration and Development System (JCIDS) to improve existing and develop new warfighting capabilities. Coordination among Department of Defense (DoD) Components is an essential element of these processes. Joint concepts and integrated architectures are used to identify and prioritize capabilities gaps and integrated Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities (DOTMLPF) solutions.***] Reference (a), paragraph 2.1, and other applicable references outline the major roles and responsibilities and provide specific processes for DON capabilities development.

For all DON capabilities identified for development, the requisite JCIDS analysis required by reference (b) must be completed. A key component of this analysis should be the use of Joint Operating Concepts, Joint Functional Concepts, and Integrated Architectures to define capability gaps, capability need, and approaches to provide the capability. Reference (c) provides guidance on interoperability and supportability of Information Technology (IT) and National Security Systems (NSS) and establishment of the Net-Ready (NR) Key Performance Parameter (KPP).

The dynamic nature of the Capabilities Development Process demands continuous communication between all participants. Changes in Capabilities Development and Acquisition Management Processes may potentially impact program cost, schedule, and performance. The timely assessment of any change, coupled with an appropriate acquisition strategy adjustment, may be vital to the preservation of an acquisition timeline.

2.1.1 DON Principal Capabilities Points of Contact

2.1.1.1 Chief of Naval Operations (CNO)/Commandant of the Marine Corps (CMC) Responsibilities

2.1.1.2 Navy Program and Resource Sponsor Responsibilities

2.1.1.3 Deputy CNO (Integration of Capabilities and Resources) (CNO (N8)) Responsibilities

2.1.1.4 Deputy CNO (Communications Networks) (CNO (N6)) Responsibilities

2.1.2 DON Capabilities Development and Processing Procedures

2.1.2.1 Naval Capabilities Development Process

For Navy Capabilities, use the NCDP, identify programming for operational capabilities and formulate an Integrated Capabilities Plan (ICP). Use the ICP to develop a subsequent Sponsor Program Proposal (SPP) detailing systems required to deliver the warfighting capabilities identified in the ICP.

2.1.2.2 Marine Corps Capabilities Development Process for Programs with Navy Fiscal Sponsorship

For Marine Corps capabilities, use the EFDS process outlined in reference (d) to formulate an Expeditionary Maneuver Warfare Capability List (ECL). The ECL provides the basis to develop Marine Corps campaign and implementation plans that are assessed and analyzed through the DOTMLPF process to identify systems required to deliver the warfighting capabilities to meet mission needs.

2.1.2.3 Weapon and Information Technology Systems Capabilities Development and Processing Procedures

Skills-based human performance requirements should be identified, developed in compliance with the Sharable Content Object Reference Model (SCORM), and grouped to form the basis for capability based and competency driven structured learning methodologies necessary to improve human performance.

2.1.2.3.1 Initial Capabilities Documents (ICDs)

Navy ICDs generated outside of OPNAV will be submitted to CNO (N810) for Navy staffing.

Once the program sponsor accepts sponsorship of the ICD, it will be processed per OPNAV procedures summarized in paragraph 2.1.2.3.3 and subsequent paragraphs and reference (e).

2.1.2.3.2 Capability Development/Production Documents (CDD/CPDs)

A CDD captures the proposed program information necessary to develop an affordable increment of capability that is useful, supportable, and that can be effectively developed, produced or acquired, deployed and sustained. The CDD is the sponsor's primary means of defining authoritative, measurable and testable capabilities needed by the warfighters to support the System Development and Demonstration phase of an acquisition program. By referencing the originating ICD and other overarching DOTMLPF changes necessary to meld the Family of Systems (FoS) and System of Systems (SoS) into an effective capability, the CDD outlines the overall strategy to develop the full or complete capability. A CDD must be validated and approved before each Milestone B decision.

An Analysis of Alternatives (AoA) normally leads the development of the CDD. The AoA and CDD may be developed and updated in parallel. However, since the final CDD should be consistent with the AoA, the AoA results should be available for inclusion in the CDD to allow for CDD independent validation efforts. Thus, the minimum acceptable operational requirements (i.e., thresholds) and objectives in the CDD will be consistent with the AoA results for program initiation. If an AoA has not been conducted, an explanation and an electronic copy of whatever alternative analysis has been performed (or planned) will be made available.

The CPD captures the production attributes and quantities specific to a single increment of an acquisition program, and is issued when the projected capabilities of that increment have been identified during the System Development and Demonstration phase with sufficient accuracy to begin production. A CPD must be validated and approved before each Milestone C decision.

References (b) and (e) provide the guidance for DON development of the CDD/CPD. Program sponsors will consider time-phased requirements in the development of CDDs in order to reduce cycle time for technology insertion, acquisition, deployment, and modernization of weapon systems and information technology systems. References (b) and (e) also provide guidance for Marine Corps program CDD/CPD development.

2.1.2.3.3 ICD/CDD/CPD Formulation

The program sponsors will accomplish the following in the preparation of DON capability documents:

1. Administer/track processing of initial capabilities proposals.

2. For ICD development, determine if any non-materiel alternatives exist.

3. For CDD/CPD development, verify that the exit criteria for the approaching milestone decision have been met.

4. Prepare draft ICDs/CDDs/CPDs per reference (e), enclosures E/F/G, respectively, Appendix A (content/format). Marine Corps programs will be forwarded by the Commanding General, Marine Corps Combat Development Command (CG, MCCDC).

6. Coordinate with the Program Executive Officer (PEO)/Systems Command (SYSCOM) Commander/Direct Reporting Program Manager (DRPM)/Program Manager (PM) or the cognizant Deputy Assistant Secretary of the Navy (Research, Development and Acquisition) (DASN(RD&A)) to verify the potential acquisition category (ACAT).

7. Coordinate with CNO (N810) before staffing to ensure appropriate OPNAV review/endorsement boards are identified (see Annex 2-A for Navy Requirement/Capability Documents Flow and Annex 2-B for Initial Capabilities/Capability Development/Production Document Signature Page). Ensure that the document complies with requirement for development/production and content (see reference (e) and Annexes 2-C and 2-D).

8. For Capability Documents (CDDs/CPDs), ensure that performance parameters satisfy the mission need and KPPs and Key System Attributes (KSAs) are clearly identified so they may be extracted and included in the Acquisition Program Baseline (APB).

2.1.2.3.4 Navy Capabilities Document Flow Process

The goal of the JCIDS document flow process is to facilitate efficient routing of capabilities documents while providing a high quality set of requirements. The OPNAV Staff has reviewed the joint and Navy capabilities documents routing process to make improvements for better support and more timely validation and approval of these documents.

Reference (b) establishes the JCIDS process and identifies document staffing guidelines. Reference (a) delineates the JCIDS document validation and approval process within the Navy. Per reference (a), Navy capability documents are required to be validated and approved by CNO and the Joint Requirements Oversight Council (JROC) for ACAT level I/IA programs, VCNO for

ACAT II through IV JROC Interest programs, and by CNO (N8) for ACAT level II and below programs that are not JROC Interest.

2.1.2.3.4.1 Roles and Responsibilities

1. Resource Sponsor

Upon receipt, the resource sponsor's action officer (AO) will expeditiously route the capabilities document package through the sponsor's organization for signature, with timely updates on its status to the designated CNO (N810) representative.

2. CNO (N810)

The designated CNO (N810) representative will staff all capability documents through the Navy and Joint organizations for review, and assist in coordinating Navy reviews (Naval Capabilities Board (NCB) and Resources and Requirements Review Board (R3B)), and Joint Staff reviews (Functional Capabilities Boards (FCBs), Joint Capabilities Boards (JCBs), and JROCs) as required. CNO (N810) will also staff Navy capabilities documents through the appropriate organizations for signature. Performance metrics will be maintained to track routing of all Navy JCIDS documents and to compare progress with JCIDS document staffing/routing guidelines.

3. CNO (N8)

Using the R3B/NCB, validates Navy JCIDS documents. Recommends approval for document entry into joint staffing to the VCNO/CNO and endorses the document for final VCNO/CNO approval after joint comment resolution.

2.1.2.3.4.2 Joint Capabilities Integration and Development System (JCIDS) Document Routing and Review Process

The staffing, signature, and final review process for Navy requirements/capabilities documents is shown in Annex 2-A.

1. Process for Navy Review

a. Program sponsor will:

(1) Submit Navy capabilities documents to CNO (N810) for distribution to the appropriate CNO staff codes for review. CNO (N810) distribution will include Commander, Fleet Forces Command (CFFC) for Fleet review.

(2) OPNAV sponsor will forward a copy of the draft capabilities documents to ASN(RD&A), ASN(RD&A) Chief Systems

Engineer (CHSENG), DASN(RD&A)(International Programs)(IP), and cognizant DASN(RD&A) and PEO/SYSCOM/DRPM for information.

(3) The notional timeframe for Navy review is 21-calendar days. The review period is followed by a 15-calendar day sponsor comment adjudication period.

(4) Communication with CNO (N810) early and frequently during the staffing process is key to successful and timely staffing of these capabilities documents. Notionally, the staffing, signature, and review process takes about 6 months for JROC Interest documents. CNO (N810) will:

(a) Conduct an initial review of capabilities documents.

(b) Enter draft capabilities documents into the Navy capabilities document tracking database.

(c) Receive comments from the Navy Staff and CFFC and provide these comments to the sponsor.

b. Naval Capabilities Board (NCB)/Resources and Requirements Review Board (R3B)

(1) The NCB/R3B will review and validate all Navy JCIDS documents. Prior to this review, the FORCEnet requirements must be certified by CNO (N6F).

(2) Signature by CNO (N8) will suffice for all 3-star endorsements of Navy JCIDS documents.

2. <u>Process for Joint Review</u>

a. CNO (N810) will:

(1) Verify final document compliance and that all endorsements (FORCEnet/NCB/R3B) are received.

(2) Forward JCIDS documents to the Joint Staff J-8 for review and receipt of Joint certifications, as required. Per JROCM 100-05, a single-phase review will suffice unless the J-8 requires a second phase, Flag level staffing and review. Reference (b) covers the JCIDS Joint staffing process, which encompasses a 21-day review and 30-day sponsor resolution period (may be extended to 45 days by the lead FCB).

3. <u>Final Navy Approval</u>

a. After sponsor resolution of comments, the document will be reviewed by the NCB/R3B, as necessary, to review any

changes that might change Navy equities in the document or is contrary to Navy leadership direction/decisions regarding that document.

b. CNO (N8) endorses applicable Marine Corps program ICD/CDD/CPDs (Assistant Commandant of the Marine Corps (ACMC) approves). At the R3B Executive Secretary's discretion, the document may bypass the R3B and go straight to CNO (N8) for endorsement. CNO (N810) will forward endorsed ICD/CDD/CPD to CMC (Deputy Commandant of the Marine Corps (Combat Development and Integration (DC,CD&I))) for ACMC review and approval for applicable Marine Corps programs.

c. The NCB/R3B validates all Navy non-JROC Interest capabilities documents, and endorses JROC Interest capabilities documents. JROC Interest documents are forwarded to CFFC, Vice Chief of Naval Operations (VCNO) and CNO for 4-star approval.

4. <u>Joint Staff Validation Approval</u>

At the conclusion of the Navy comment resolution period, CNO (N810) will post the document in the J-8 Knowledge Management/Decision System (KM/DS) as an FCB draft. Navy 4-star signatures are required prior to JCB and JROC review and approval (ACAT I through IV JROC Interest documents only). Reference (b) and JROCM 100-05 apply for Joint Staffing of JCIDS documents.

5. <u>JROC Interest Endorsement</u>

a. NCB/R3B will:

(1) Review and endorse ICD/CDD/CPD (Navy and applicable Marine Corps programs).

(2) Forward ICD/CDD/CPD to VCNO for review.

b. VCNO will:

(1) Review, validate, and endorse Navy ACAT II through IV JROC Interest ICD/CDD/CPDs. VCNO will review applicable Marine Corps programs.

(2) Forward ACAT I JROC Interest ICD/CDD/CPDs to CNO for review, Navy validation and approval.

(3) Review and comment as needed on proposed JROC briefing (Navy programs only).

c. CNO will review, validate, and endorse ACAT I/IA ICD/CDD/CPDs for Navy prior to the JCB. CNO will review applicable Marine Corps programs prior to the JROC.

6. <u>JROC Validation and Approval of ACAT I/IA and JROC Interest Programs</u>

a. CNO (N810) will:

(1) For Navy programs, coordinate with program sponsor to provide JROC briefings (FCB, JCB, and JROC) following the Navy process and monitor progress of JROC Interest ICD/CDD/CPD validation and approval.

(2) For applicable Marine Corps programs, forward N8 endorsement to CMC (DC,CD&I), as applicable.

7. <u>Issuance</u>

a. CNO (N810) will:

(1) Serialize ICD/CDD/CPD (M____-[Sponsor N-code]-CY) and post the document to the J-8 Knowledge Management/Decision System (KM/DS).

(2) Retain the document for configuration management/archive purposes.

b. The program sponsor will:

(1) Forward the ICD/CDD/CPD to ASN(RD&A) for potential ACAT I/IA or potential ACAT II designation, or PEO/SYSCOM/DRPM for potential ACAT III or IV designation, and initial milestone scheduling.

c. ASN(RD&A) will:

(1) Forward potential ACAT I/IA ICDs to USD(AT&L)/ASD(NII) for designation and initial milestone scheduling.

(2) Forward the approved CDD/CPD to the Milestone Decision Authority (MDA) and PM.

d. MDA will:

(1) Schedule a milestone meeting.

2.1.2.3.5 <u>Navy Capabilities Document Change Process</u>

Over time changes to capabilities documents may be required. Reasons for document changes may range from revised KPP criteria to small administrative changes. The previous capabilities document routing system did not contain a change process. Therefore, all changes to capabilities documents were subject to a full review by all organizations that participated in the initial document review. This policy has led to a reactive practice whereby documents are not updated until new or

revised requirements are issued that mandate immediate or timely updating of capabilities documents. The result of this practice has been capability documents that do not reflect all of the current requirements and difficulty in keeping documents current for minor requirement changes, without an extensive review.

Realizing that some capabilities document changes may be less critical than others, the change process is based on the type of change and the category of the document and has different document staffing and approval requirements. The staffing and approval levels of capabilities document changes may differ based on the joint potential designator (JPD) of the capabilities document. (See reference (b) for description of JPDs). The document change criteria include three categories as follows.

2.1.2.3.5.1 Changes to Key Performance Parameter (KPP) Requirements

KPP changes may result from (1) schedule changes to delivering the capability, (2) requirements changes as a program matures, (3) de-scoping of requirements, and (4) CDD/CPD/ Operational Requirements Document (ORD) clarifications.

1. For capabilities documents with a JPD of "JROC Interest," changes must be staffed through all Navy and other service codes. Approval authority for these changes is the JROC.

2. For capabilities documents with a JPD of "Joint Integration," changes must be staffed through all Navy and other service codes. Approval authority for these changes is CNO (N8)/VCNO depending on the change and ACAT level.

3. For capabilities documents with a JPD of "Joint Information" changes must be staffed through all Navy codes. Approval authority for these changes is CNO (N8).

4. For capabilities documents with a JPD of "Independent" changes must be staffed through all Navy codes. Approval authority for these changes is CNO (N8).

2.1.2.3.5.2 Changes to Key System Attributes (KSAs)

2.1.2.3.5.3 Changes to Non-Key Performance Parameters (Non-KPPs) or Non-Key System Attributes (Non-KSAs)

Non-KPP/KSA changes may result from the same four causes for KPP changes: (1) schedule changes to delivering the capability, (2) requirements changes as the program matures, (3) de-scoping of requirements, and (4) CDD/CPD/ORD clarifications.

1. For capabilities documents with a JPD of "JROC Interest," changes must be staffed through all Navy codes. Approval authority for these changes is the VCNO.

2. For capabilities documents with a JPD of "Joint Integration," changes must be staffed through all Navy codes. Approval authority for these changes is CNO (N8).

3. For capabilities documents with a JPD of "Joint Information," changes must be staffed through all Navy codes. Approval authority for these changes is CNO (N8).

4. For capabilities documents with a JPD of "Independent," changes must be staffed through all Navy codes. Approval authority for these changes is CNO (N8).

2.1.2.3.5.4 Administrative Changes

Administrative changes may only result from CDD/CPD/ORD clarifications. Approval authority for these changes is CNO (N81D).

2.1.2.3.5.5 Staffing and Approval Matrix for Changes to Capability Documents

Table E2T1 matrix below provides an illustration of staffing and approval requirements for changes to capabilities documents.

Table E2T1 Staffing and Approval of Changes to Capabilities Documents			
Joint Potential Designator	**Change Type**	**Staffing**	**Approval**
JROC Interest			
KPP	Schedule Change for Delivering Capability	Navy Staffing (including NCB/R3B), Joint Staffing	JROC
	Requirements Change as Program Matures		
	Descoping Requirement		
	CDD/CPD/ORD Clarification		
Non-KPP Rqmts (to include KSA changes)	Schedule Change for Delivering Capability	Navy Staffing, NCB/R3B	VCNO/CNO
	Requirements Change as Program Matures		
	Descoping Requirement		
	CDD/CPD/ORD Clarification		
Admin	Administrative change only	N810	N81D
Joint Integration			
KPP	Schedule Change for Delivering Capability	Navy Staffing (including NCB/R3B), Joint Staffing	N8
	Requirements Change as Program Matures		
	Descoping Requirement		
	CDD/CPD/ORD Clarification		
Non-KPP Rqmts (including KSA changes)	Schedule Change for Delivering Capability	Navy Staffing, NCB/R3B	N8
	Requirements Change as Program Matures		
	Descoping Requirement		
	CDD/CPD/ORD Clarification		
Admin	Administrative change only	N810	N81D
Joint Information and Independent			
KPP	Schedule Change for Delivering Capability	Navy Staffing, NCB/R3B	N8
	Requirements Change as Program Matures		
	Descoping Requirement		
	CDD/CPD/ORD Clarification		
Non-KPP Rqmts (including KSA changes)	Schedule Change for Delivering Capability	Navy Staffing, NCB/R3B	N8
	Requirements Change as Program Matures		
	Descoping Requirement		
	CDD/CPD/ORD Clarification		
Admin	Administrative change only	N810	N81D

2.1.2.4 Fleet Modernization Program

Submitters of Ship Maintenance (SHIPMAIN) Ship Change Documents (SCDs) should use the operational requirements/ capabilities language from JCIDS documents. Submitters of a SCD for ship modernization should coordinate with Program Managers (PMs) to ensure that the cost data reported in the Cost Benefit Analysis (CBA) form of the SCD originates from the program's independent cost analysis. The CBA data should be consistently reflected in the associated APB.

2.1.2.5 FORCEnet

FORCEnet capabilities are described by the FORCEnet Functional Concept of 7 Feb 05. The Navy FORCEnet Requirements/Capabilities and Compliance (FRCC) Flag Board and Marine Corps Command, Control, Communications, Computers, and Intelligence (C4I) Integration Board provide guidance for IT systems, including NSS, FORCEnet requirements and capabilities compliance with the current FORCEnet Consolidated Compliance Checklist (FCCC).

Compliance of individual IT systems, including NSS, with joint interoperability guidance is critical for DON transformation to a Net-Centric Operations and Warfare (NCOW) environment; this is a primary focus of FORCEnet. The FCCC includes FORCEnet capabilities/requirements system, technical, and policy criteria. The FCCC is a distillation of relevant DoD and DON joint, net-centric guidance, including enterprise-wide FORCEnet integrated architectures and standards. An example of the FCCC is available in this guidebook, enclosure (2), Annex 2-E, at the DON Research, Development and Acquisition website. The FCCC is updated and maintained using the CNO FRCC process that is integrated with the NCDP and JCIDS processes. The FRCC process is described, and the FCCC is available, in CNO (N6/N7) FRCC memorandum of 27 May 05.

CNO program and resource sponsors are responsible for identifying and defining FORCEnet requirements/capabilities in the current FCCC, and for ensuring FORCEnet compliance via synthesis of FCCC requirements/capabilities criteria into Navy JCIDS capabilities documents during development and review of these documents, and into programming decisions made during the NCDP.

The Global Information Grid Mission Area Initial Capabilities Document (GIG MA ICD), an element of the FCCC in Annex 2-E, provides direction for all DoD and Intelligence Community Components in developing CDDs and CPDs. Appendix F of the GIG MA ICD is a checklist for program/resource sponsors to use in completing a capability requirements crosswalk to ensure compliance with the GIG MA ICD. For new IT systems, including NSS, and for upgrading legacy IT systems, including NSS, the GIG

MA ICD also provides guidance for future FORCEnet IT systems, including NSS, investments to ensure interoperability.

The Commander, Naval Network Warfare Command (NETWARCOM) and the CG, MCCDC in support of their respective Navy and Marine Corps program and resource sponsors are developing enterprise-wide FORCEnet integrated architecture operational views (OVs) during the development of IT, including NSS, JCIDS capabilities documents. NETWARCOM supports program and resource sponsors during the NCDP process using the FORCEnet Enterprise Team (FET).

Space and Naval Warfare Systems Command (COMSPAWARSYSCOM) (FORCEnet Chief Engineer (CHENG)) leads the development of enterprise-wide FORCEnet integrated architecture System Views (SVs) and Technical Views (TVs) for support of program and resource sponsors' preparation of IT, including NSS, JCIDS capabilities documents per reference (c). COMSPAWARSYSCOM (FORCEnet CHENG) supports program and resource sponsors during the NCDP process and PMs during the acquisition process using the FCCC criteria. Approved DON-wide Enterprise FORCEnet integrated architectures are available on the DOD Architecture Repository System (DARS) website at https://dars1.army.mil/.

2.1.2.5.1 FORCEnet Requirement/Capabilities and Compliance Process

Figure 1 illustrates the FRCC process that updates and validates the FCCC. The FRCC is composed of the following steps:

1. Collection of pertinent top-level guidance.

2. Review of top-level guidance and proposed FCCC updates and identification of issues by a CNO (N6F)-chaired FRCC Review Board consisting of senior/O-6 level representatives from OPNAV, Naval NETWARCOM, ASN(RD&A) CHSENG, DON CIO, COMSPAWARSYSCOM (FORCEnet CHENG), and other organizations invited by CNO (N6F). A senior representative from the Marine Corps will also participate as a liaison to the FRCC Review Board to ensure alignment of FORCEnet policy and implementation across both Services.

3. Resolution of FCCC issues by a FRCC Flag Review Board, chaired by CNO (N6F) and consisting of Flag/SES-level FORCEnet stakeholders as invited by CNO (N6F).

4. Approval of FRCC Flag Board recommended updates to the FCCC by CNO (N6) (FORCEnet sponsor). An example of the FCCC is provided in Annex 2-E. An FCCC, as well as the supporting FRCC policy and all FCCC reference documents, is available in CNO (N6/N7) FRCC memorandum of 27 May 05.

FORCEnet Requirements/Capabilities and Compliance (FRCC) Process

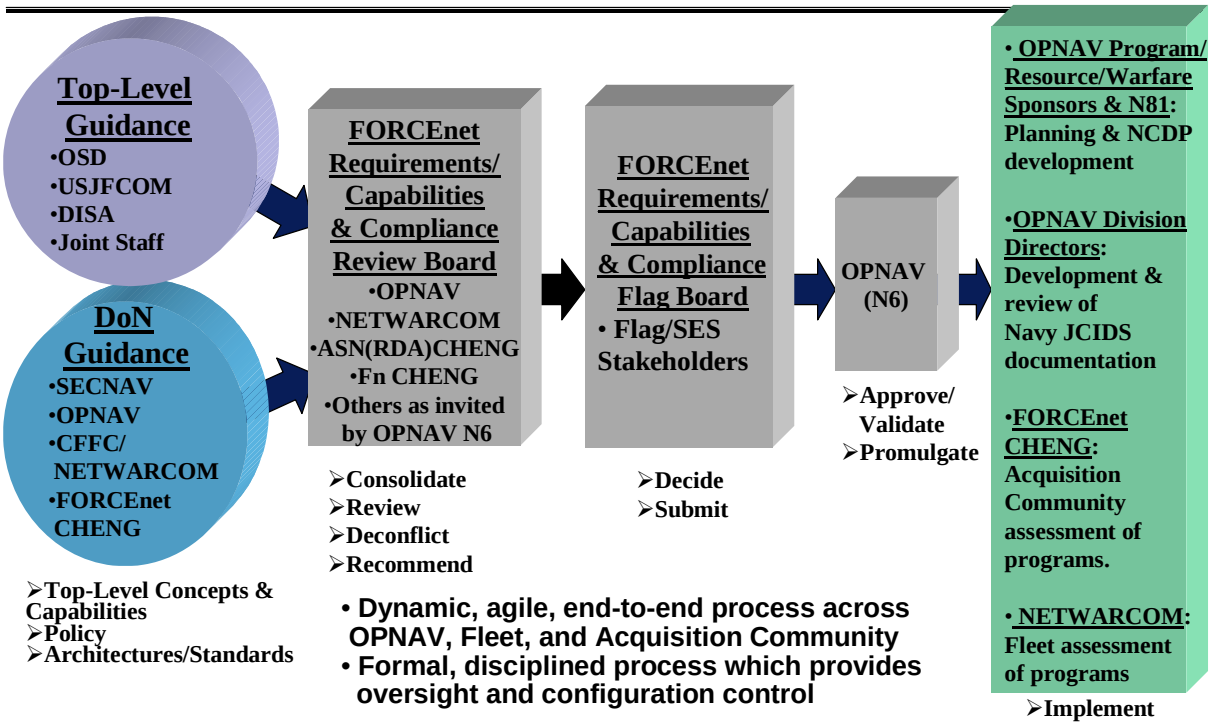


Figure 1 (see acronyms in Enclosure (12))

FORCEnet Requirements/Capabilities and Compliance Process

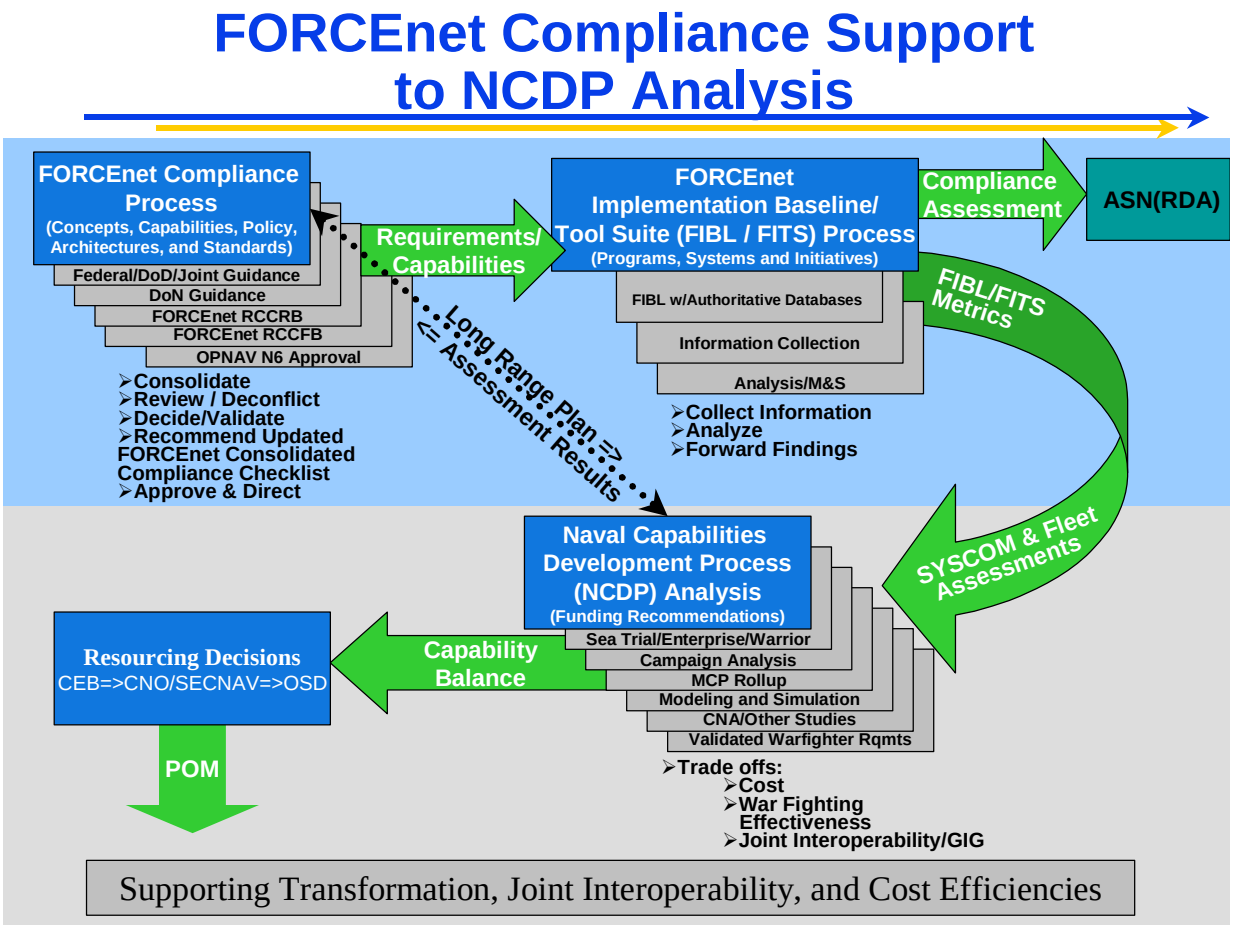


Figure 2 (see acronyms in Enclosure (12))

FORCEnet Compliance Support to Naval Capabilities Development Process (NCDP) Analysis

2.1.2.5.2 Support to Naval Capabilities Development Process

1. The NCDP was developed to transform a threat-based, platform-centric requirements process into a capabilities-based assessment measured against "what it takes to win." The NCDP uses FORCEnet capabilities to assess program necessity, requirements, gaps, and overlaps, and provides a fiscal AoA for achieving FORCEnet capabilities utilizing modeling and simulation, experimentation, science and technology, wargames, and lessons learned. The NCDP addresses the material component of FORCEnet capability.

2. The FRCC Process shown in figure 1 supports the NCDP, enhancing resource decisions by adding information on joint interoperability, GIG transition, and other key elements to the

current tradeoff of warfighting capability and cost. This support is described in figure 2 and as follows:

a. The FRCC process provides validated FORCEnet compliance criteria.

b. The COMSPAWARSYSCOM (FORCEnet CHENG)-led FORCEnet Implementation Baseline (FIBL)/FORCEnet Implementation Tool Suite (FITS) process will assess individual DON acquisition programs against FCCC criteria and assign them to categories based on their compliance. FIBL/FITS findings will also be used by COMSPAWARSYSCOM (FORCEnet CHENG) in development of the SYSCOM FORCEnet Assessment input to NCDP.

c. The results of the FIBL/FITS assessment will undergo operational review by the Fleet (NETWARCOM)-chaired FORCEnet Enterprise Team (FET). Recommendations from this review will be provided to appropriate OPNAV program and resource sponsors, identifying non-compliant systems for potential consolidation or termination in the Integrated Sponsor's Program Proposal.

2.1.2.5.3 FORCEnet Consolidated Compliance Checklist

[***fm SNI 5000.2D, 2.1.2.3 (ninth subparagraph): Program and resource sponsors shall use the current FORCEnet Consolidated Compliance Checklist (FCCC) to determine the Net-Centric Operations/Warfare (NCOW) and other applicable requirements for both tactical (warfighting) and non-tactical (business/support) IT systems, including NSS. The FCCC shall be validated, maintained and updated by CNO (N6), and is available in the CNO (N6/N7) FRCC memorandum of 27 May 05. CNO (N6) shall assist program and resource sponsors by reviewing all Navy JCIDS documents against the current FCCC to ensure that applicable FORCEnet/NCOW requirements are being correctly and consistently incorporated into these documents. COMSPAWARSYSCOM (FORCEnet CHENG) and NETWARCOM will use the current FCCC to assess individual programs for FORCEnet/NCOW compliance, and shall make appropriate reports of these assessments to CFFC, CNO (N6), and ASN(RD&A). COMSPAWARSYSCOM (FORCEnet CHENG) and NETWARCOM, using the current FCCC, shall assist Program Managers in assessing and achieving FORCEnet/NCOW compliance in their programs and shall report results of these assessments as necessary.***] The FCCC is organized in four sections: (1) FORCEnet Operational Criteria, (2) FORCEnet System and Technical Criteria, (3) FORCEnet Policy Criteria, and (4) Implementation Planning.

1. FORCEnet Operational Criteria.

a. FORCEnet Integrated Architecture. This section is based on the FORCEnet Integrated Architecture Operational Views (OVs). The FORCEnet Integrated Architecture is being aligned with the GIG Integrated Architecture and will provide products

which represent FORCEnet requirements/capabilities to support assessment of capabilities through the NCDP.

b. FORCEnet Capabilities List (FCL). Closely related to the FORCEnet Integrated Architecture is the FCL. The FCL will map and time-phase FORCEnet capabilities to Joint capabilities, attributes, and measures in the Joint Functional Concepts (Net-Centric, Command and Control, and Battlespace Awareness) and Joint Capability Areas (JCAs), providing additional alignment of FORCEnet with Joint planning and JCIDS.

2. FORCEnet System and Technical Criteria. The FORCEnet System/Technical Section points to key joint, net-centric, and GIG technical guideposts and supporting implementation guidance and direction.

3. FORCEnet Policy Criteria. The FORCEnet Policy Criteria provides a compendium of guidance in key FORCEnet policy areas.

4. Implementation Planning. This section reflects FCCC/FORCEnet implementation planning by CNO (N6) (FORCEnet sponsor) and ASN(RD&A).

2.1.2.5.4 <u>FORCEnet Compliance Governance Process</u>

FORCEnet compliance is implemented via synthesis of FORCEnet requirements/capabilities into the JCIDS process during development and review of JCIDS documents, as shown in Annex 2-A, and into the NCDP process, as shown in Figure 2. The FET process will be used to enable FORCEnet compliance in the Fleet and Operational Community. Additionally, FORCEnet compliance enforcement should be implemented in the Fleet Operational Advisory Group (OAG) process. FORCEnet compliance should be coordinated with the Sea Trial process.

2.1.2.5.5 <u>Roles and Responsibilities</u>

1. FORCEnet Enterprise Team (FET) is led by NETWARCOM, and consists of CNO (N6) (FORCEnet sponsor) and Acquisition Community representatives. The FET will:

a. Perform an operational review of the results of the FIBL/FITS program assessments by COMSPAWARSYSCOM (FORCEnet CHENG).

b. Provide program assessment recommendations to appropriate OPNAV program and resource sponsors, identifying non-compliant systems for potential consolidation or termination in the Integrated Sponsor’s Program Proposal

2. FORCEnet Requirements/Capabilities and Compliance (FRCC) Review Board is chaired by CNO (N6F) and consists of Senior/O-6 level representatives of cognizant OPNAV codes, DON

CIO, NETWARCOM, ASN (RD&A) CHSENG, COMSPAWARSYSCOM (FORCEnet CHENG), and other organizations deemed appropriate by CNO (N6F). A senior representative from the Marine Corps will also participate as a liaison to the FRCC Review Board to ensure alignment of FORCEnet policy and implementation across both Services. The FRCC will:

a. Consolidate all Top-Level and DON applicable guidance, resolve any conflicting guidance, and develop recommended changes/updates to the FCCC, which will be forwarded to the FRCC Flag Board for review.

3. FRCC Flag Board is led by CNO (N6F), and consists of Flag/SES level representatives of FORCEnet stakeholders as invited by CNO (N6F). The FRCC Flag Board will:

a. Review proposed updates to the FCCC and resolve any issues identified by the FRCC Review Board.

b. Forward recommendations to CNO (N6) (FORCEnet sponsor) for approval

4. CNO (N6) (FORCEnet sponsor) will:

a. Make any necessary adjustments to FRCC Flag Board recommendations and approve and promulgate an update of the FCCC.

b. Enforce FORCEnet compliance.

5. NETWARCOM and MCCDC are the FORCEnet Operational Agents. Responsibilities include:

a. Co-develop the FCCC FORCEnet Operational Criteria.

b. Develop the FORCEnet Integrated Architecture Operational Views (OVs) in coordination with the other FORCEnet stakeholders and OSD staff.

c. Develop the FORCEnet Capabilities List (FCL) in coordination with CNO (N6) (FORCEnet sponsor) and other FORCEnet stakeholders.

6. COMSPAWARSYSCOM (FORCEnet CHENG) (lead) with MARCORSYSCOM are the FORCEnet System and Technical Agents. Responsibilities include:

a. Co-develop the FCCC FORCEnet System and Technical Criteria.

b. Develop the FORCEnet Integrated Architecture System Views (SVs) and Technical Views (TVs) in coordination with the other FORCEnet stakeholders and SYSCOMs.

c. Ensure traceability of the FCL to system and technical documentation and implementation into the FORCEnet Integrated Architecture.

2.2 Acquisition Management Process

2.3 Overview of the Acquisition Management Process

2.3.1 Integrated Product Teams (IPTs)

2.3.1.1 Overarching Integrated Product Teams (OIPTs)

OIPTs are generally composed of SES and Flag officers with direct knowledge of DoD, DON, and Joint mission capabilities needs.

2.3.1.2 Working Integrated Product Teams (WIPTs)

ASN(RD&A) CHSENG, as the senior technical authority for DON, should be a Working IPT (WIPT) member for all ACAT I and IA programs and an Acquisition Coordination Team (ACT) member for other Acquisition Category (ACAT) programs as appropriate.

2.3.2 Acquisition Coordination Teams (ACTs)

2.4 Categories of Acquisition Programs and Milestone Decision Authorities

Annex 2-F contains the contents of a memorandum for requesting an ACAT designation or a change in ACAT designation.

2.5 Capability Concept Development and Program Decision Points and Phases

2.5.1 User Needs and Technology Opportunities

2.5.2 Program Tailoring

2.5.3 Program Decision Points Tailoring

[***fm SNI 5000.2D, 2.5.3: An ACAT program does not require a set number of program decision points.***]

As an example of decision point tailoring, it is conceivable that a Commercial-Off-The-Shelf (COTS) acquisition strategy could have program initiation at a combined Milestone C and Full-Rate Production Decision Review (FRP DR) and go directly into production or deployment. Yet there are certain core activities that must be addressed at the FRP DR such as need validation; acquisition strategy; affordability, life-cycle cost, total ownership cost, and funding adequacy; industrial base assurance per reference (f); risk assessments and risk management; interoperability and integration; compliance with the legacy joint technical architecture that has been replaced with

the DoD Information Technology Standards Registry (DISR); supportability; safety and health; environmental compliance; and operational effectiveness and suitability testing prior to an FRP decision or deployment, or subsequent to an FRP decision for modifications. Per reference (a), all of these activities shall be considered in light of the other systems (and associated programs) in a SoS or FoS and the impact of the introduction of a new program on the mission capability of a SoS or FoS.

2.5.4 Program Decision Points and Phases

2.5.4.1 Concept Decision

2.5.4.2 Concept Refinement

2.5.4.3 Milestone A

The Technology Development Strategy (TDS) discussion of the viability, feasibility, and applicability of technologies should include consideration of the Human Systems Integration (HSI) implications. The costs associated with changes to manpower, personnel, and training as a result of technology insertion should be factored into any affordability assessment analysis conducted as part of the TDS development. The availability of trained and qualified personnel to support the technology should be considered in assessments of feasibility and risk.

2.5.4.4 Technology Development

2.5.4.5 Milestone B

2.5.4.6 System Development and Demonstration

2.5.4.6.1 System Integration

2.5.4.6.2 Design Readiness Review

The PM may propose the form and content of the Design Readiness Review to the MDA at Milestone B for inclusion in the ADM.

2.5.4.6.3 System Demonstration

2.5.4.7 Milestone C

2.5.4.8 Production and Deployment

2.5.4.9 Operations and Support

2.5.4.9.1 Sustainment

2.5.4.9.1.1 Sustainment Support

See ASN(RD&A) memorandum of 27 Jan 03 for Performance Based Logistics sustainment support guidance.

2.5.4.9.2 Disposal

As the total life cycle manager, PMs consider and plan for the ultimate demilitarization and disposal of the system. The PM considers materiel demilitarization and disposal during systems engineering. The PM carefully considers the impacts of any hazardous material component requirements in the design stage to minimize their impact on the life cycle, including storage, packaging, handling, transportation and disposition. The PM coordinates with Service logistics activities, Defense Logistics Agency (DLA), and CNO (N43) and Naval Sea Systems Command (NAVSEA)/Supervisor of Shipbuilding, as appropriate, to identify and apply applicable demilitarization requirements necessary to eliminate the functional or military capabilities of assets (see DOD 4140.1-R, DoD Supply Chain Materiel Management Regulation, and DOD 4160.21-M, Defense Materiel Disposition Manual).

The U.S. Department of Labor, Occupational Safety and Health Administration (OSHA), has a National Emphasis Program on shipbreaking (ship scrapping), using industry best practices and electronic Compliance Assistance Tools (eCATs) that are available on the OSHA web page at http://www.osha.gov. The National Institute for Occupational Safety and Health (NIOSH), the occupational safety and health research arm of OSHA and the U.S. Department of Health and Human Services, Centers for Disease Control (CDC), are establishing a comprehensive listing of industry best practices for ergonomic interventions in the building, repair, and dismantling of ships that is available on the NIOSH web page at http://www.cdc.gov/niosh/ergship/ergship.html. See reference (g), enclosure 2, paragraph 8c(2), and DOD 4140.1-R and DOD 4160.21-M for demilitarization and disposal implementation requirements for DON ACAT programs.

2.5.5 Modifications

2.6 Review of the Legality of Weapons Under International Law and Compliance with Arms Control Agreements

2.7 Non-Acquisition Programs

Examples of non-acquisition programs are:

1. Science and Technology Programs.

a. Technology based programs in basic research (RDT&E category 6.1) and applied research (RDT&E category 6.2).

b. Advanced technology development (RDT&E category 6.3).

2. Developmental or operational assessment of developmental articles, concepts, and experiments funded by RDT&E category 6.4, 6.5, or 6.7 funding and with **no** directly related acquisition program effort.

3. Management and support of installations or operations required for general-purpose research and development use (included would be test ranges, maintenance of test aircraft and ships, and studies and analyses **not** in support of a specific acquisition program research and development effort) funded by RDT&E category 6.6 funding.

2.7.1 Management of Non-Acquisition Programs

Non-acquisition programs will be managed as follows:

Non-acquisition programs that are outside of the Future Naval Capability (FNC) and Innovative Naval Prototype (INP) review process will be reviewed annually by OPNAV sponsors/CMC (DC,CD&I) to verify that such programs are pursuing valid Naval requirements and are executing per the applicable Research and Development Descriptive Summary (RDDS). The results of these annual reviews will be made available for subsequent Program Objective Memorandum (POM) development. Non-acquisition programs that are FNC projects will be reviewed annually through the FNC process.

Non-acquisition programs will use documentation required to support the Planning, Programming, Budgeting, and Execution System (PPBES).

Navy requests to initiate a non-acquisition program funded by RDT&E categories 6.4 - 6.7 will be submitted to a CNO resource sponsor by PEOs, SYSCOMs, DRPMs, or any other appropriate DON activity. Marine Corps requests to initiate a non-acquisition program funded by RDT&E categories 6.4 - 6.7 will be submitted to CMC (Deputy Commandant, Programs and Resources (DC,P&R)).

Approval of non-acquisition programs will be provided by CNO (N6/N8) or CMC (DC,CD&I). CNO (N6/N8)/CMC (DC,CD&I) approval constitutes commitment for the effort.

Deliverables from non-acquisition programs that transition into a related ACAT program should be identified in an AoA, a capability development/production document (CDD/CPD), and an APB for that ACAT program. Guidance about technology transition is provided in the DUSD(S&T) document, "Technology Transition for Affordability, *A Guide for S&T Program Managers*" of April 2001 and OUSD(AT&L)DP&AP document, "Manager's Guide to Technology Transition in an Evolutionary Acquisition Environment Version 1.0 of 31 January 2003." These documents can be accessed at https://www.dodmantech.com/pubs/TechTransGuide-Apr01.pdf and

http://www.acq.osd.mil/jctd/articles/AQ201S1v10Complete.pdf, respectively.

Per reference (a), a listing of all approved non-acquisition programs shall be provided to ASN(RD&A) annually by CNO (N6/N8)/CMC (DC,CD&I).

2.8 Rapid Deployment Capability (RDC) Process and Procedures

2.9 Executive Review Procedures

2.9.1 DON Program Decision Process

Per reference (a), recommendations to the MDA regarding program continuance shall address logistics and sustainment factors in balance with other major decision factors. Per reference (a), for joint Service programs where the Navy or Marine Corps is the lead or joint program manager (including joint Service programs where the Navy or Marine Corps is the executive, participating, or lead Service) responsible for introducing systems to be operated, maintained, and/or supported by Navy or Marine Corps forces, independent logistics assessments shall be conducted and the results of the assessments certified for the planned Navy/Marine Corps assets.

2.9.2 Information Technology (IT) Acquisition Board (ITAB) Reviews

2.9.3 Defense Space Acquisition Board (DSAB) Reviews

2.9.4 Defense Business System Management Committee (DBSMC) Certification and Approval

2.9.4.1 Defense Business System Definition

2.9.4.2 Roles and Responsibilities

2.10 Source Selection Authority (SSA)

2.10.1 ACAT I, IA, and II Programs

2.10.2 ACAT III, IV, and Abbreviated Acquisition Programs

2.10.3 Other Competitively Negotiated Acquisitions

2.10.4 Source Selection Advisory Council (SSAC)

An SSAC will consist of a chair, appointed by the SSA, and other senior military and civilian personnel, appointed by the SSAC Chair, to act as advisors throughout the source selection process. The SSAC Chair will ensure that Source Selection Evaluation Board (SSEB) members are adequately trained with respect to the statement of work, evaluation criteria, evaluation methodology, current procurement laws, and documentation

requirements. The SSAC will normally include representatives from the various functional areas involved in the procurement. While not an SSAC member, legal counsel normally will be available to advise the SSAC. The SSAC will ensure the evaluation was conducted and documented per the Source Selection Plan and will prepare a written source selection recommendation for the SSA.

2.10.5 Source Selection Evaluation Board (SSEB)

An SSEB will consist of a chair, appointed by the SSAC Chair, and other qualified Government contracting, technical and administrative/management personnel appointed by the SSEB Chair, to direct, control and perform the evaluation of proposals and to produce facts and findings required in the source selection process. A technical evaluation team composed of knowledgeable and professionally competent personnel in appropriate specialty areas may assist an SSEB. Such personnel should have previous experience in similar or related programs so as to provide mature judgment and expertise in the evaluation. Non-government personnel may not be members of an SSEB. While not an SSEB member, qualified legal counsel, different from an SSAC legal counsel, normally should be available to advise an SSEB.

2.10.6 ASN(RD&A) Source Selection Briefing

For ACAT I and II programs, the SSA will ensure that ASN(RD&A), or cognizant DASN, is briefed on the principal results of the source selection decision prior to contract award(s) and prior to the public announcement of such award(s).

2.11 Two-Pass/Six-Gate DON Requirements and Acquisition Governance Process

2.11.1 Purpose

2.11.2 Objective

2.11.3 Scope and Appliability

2.11.4 Organization and Procedures

2.11.4.1 Concept Decision and Concept Refinement Phase

2.11.4.1.1 Pass 1

2.11.4.1.1.1 Gate 1

2.11.4.1.1.2 Gate 2

2.11.4.1.1.3 Gate 3

2.11.4.2 Milestone A and Technology Development Phase

2.11.4.2.1 Pass 2

2.11.4.2.1.1 Gate 4

2.11.4.3 Milestone B and System Development and Demonstration Phase

2.11.4.3.1 Pass 2

2.11.4.3.1.1 Gate 5

2.11.4.3.1.2 Gate 6

2.11.4.4 DON Requirements/Acquisition Gate Review Membership

2.11.4.4.1 Chairperson

2.11.4.4.2 Principal Members

2.11.4.4.3 Advisory Members

2.11.4.5 DON Requirements/Acquisition Individual Gate Membership and Input/Exit Criteria

2.11.4.6 System Design Specification (SDS) Description

2.11.5 Responsibilities

2.11.5.1 ASN(RD&A)

2.11.5.2 CNO/CMC

2.11.5.3 DCNO (N8)/DC, CD&I

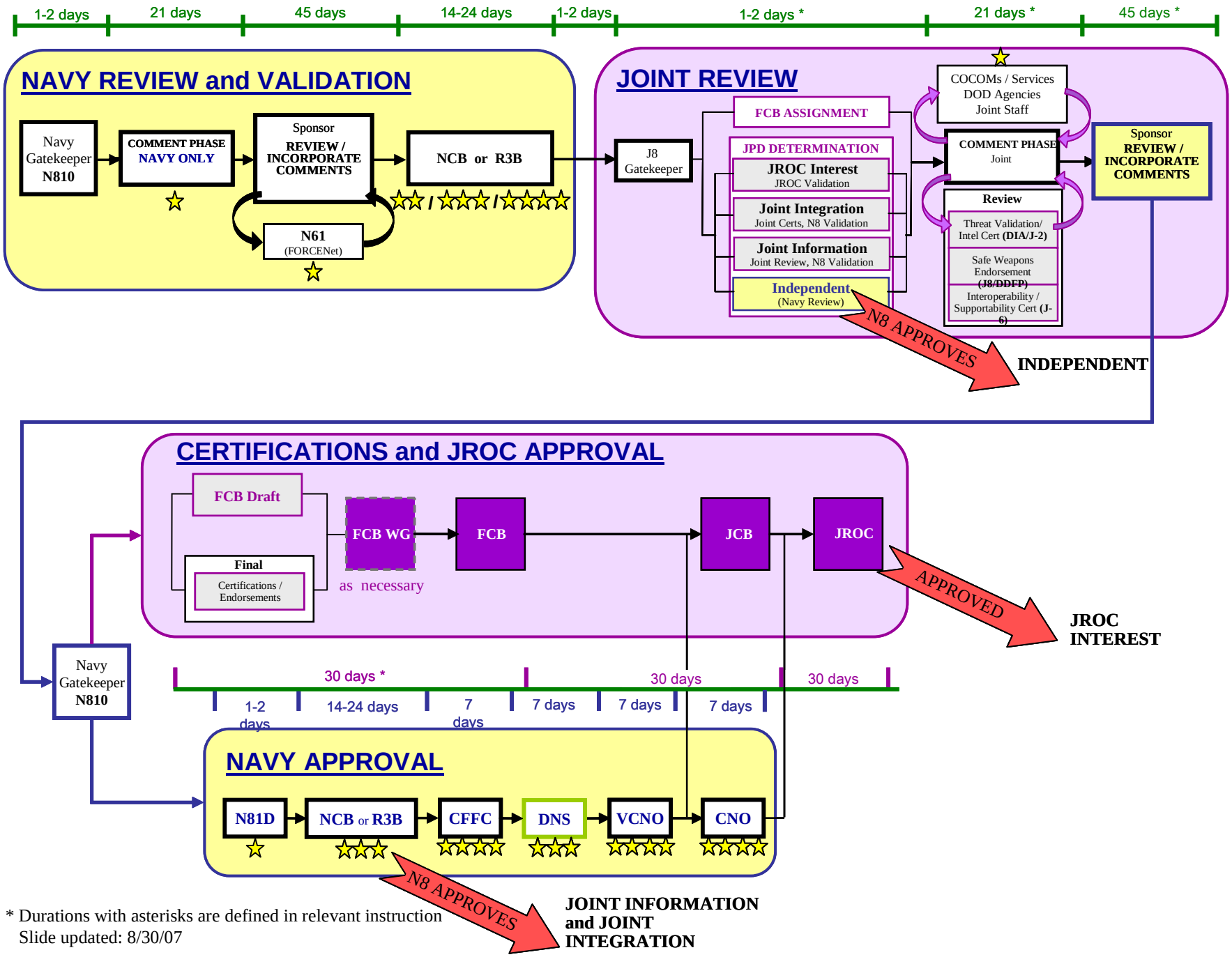
2.11.5.4 PEOs/SYSCOMs

2.11.5.5 ASN(FM&C)FMB

2.11.5.6 OGC

2.11.6 Industry Involvement

Annex 2-A Navy Requirement/Capability Documents Flow



* Durations with asterisks are defined in relevant instruction
Slide updated: 8/30/07

Annex 2-B
Initial Capabilities/Capability Development/Production Document Signature Page
(Insert Document Type Here)
FOR
[TITLE OF PROGRAM]
(POTENTIAL ACAT LEVEL ____/UPCOMING MILESTONE ____)
Serial Number (*): _____

SUBMITTED:

_____ _____
(PROGRAM SPONSOR) (DATE)

ENDORSED and FORWARDED:

_____ _____
(N6F) (FORCEnet Compliance) (DATE)

_____ _____
(N81D) (DATE)

APPROVED and VALIDATED: (JOINT INTEGRATION and Below)

_____ _____
(N8F) (NCB Chair, as required) (DATE)

_____ _____
(N8) (R3B Chair) (DATE)

REVIEWED:

_____ _____
(CFFC N00) (DATE)

_____ _____
(VCNO) (DATE)

APPROVED and VALIDATED: (JROC INTEREST)

_____ _____
(CNO) (*/**) (DATE)

_____ _____
(JROC) (*/**) (DATE)

[Guide only. Actual format to be tailored by program sponsor and CNO (N810)]

(*) - CNO (N810) will assign serial number once validated and approved. For ACAT ID programs, CNO (N810) will insert JROC validation and approval date prior to issuance.

(**) - JROC validates and approves unless delegated. The signature page will be tailored accordingly.

Annex 2-C
Initial Capabilities Document (ICD) Content Guidance

See reference (e), enclosure E, appendix A, for mandatory initial capabilities document (ICD) format.

Reference (e), enclosure E, appendix A, **ICD format paragraphs/sections 6a, 6b, 7b, and 7c**, will be implemented for Navy systems as amplified below in this annex.

6. Functional Solution Analysis Summary

a. Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities (DOTMLPF) Analysis

The DOTMLPF analyses should summarize the conclusion of the analyses conducted during the Functional Area Analysis (FAA), Functional Needs Analysis (FNA) and Functional Solution Analysis (FSA) and explain if changes in manpower, personnel and training concepts, policy and practices could be implemented to meet the deficiency. It should also summarize whether accomplishment of minor human factors engineering modifications to existing systems could enhance current system performance enough to meet the deficiency within the required safety, personnel survivability and habitability requirements. Discussion of these analyses, and reasons why changes in DOTMLPF/Human Systems Integration (HSI) will not satisfy the need, should be specific. A blanket statement that DOTMLPF changes alone will not satisfy the deficiencies is neither useful nor adequate.

b. Ideas for Materiel Approaches

Proponents should consult with the Navy IPO for assistance and guidance in meeting the reference (b) requirements for examination of existing or future allied military systems and for recommended approaches to including international considerations in the materiel approach.

7. Final Recommendations

a. (no additional guidance)

b. Per reference (e), HSI constraints that impact concept feasibility, total system performance and affordability shall be included in Section 7b of the ICD as key boundary conditions of the Analysis of Alternatives (AoA).

c. Section 7c of the ICD should describe the DOTMLPF and policy implications and constraints to include all HSI domains. Examples of HSI implications and constraints may include: end-strength limitations for manpower; affordability of developing

and training new Knowledge, Skills and Abilities (KSAs) not currently available in the Navy personnel inventory; minimums and appropriate mix of manpower (military, civilian and contractor), and environmental regulations and workspace safety compliance requirements. Other HSI-related information relevant to system design should be provided as guidance in these sections of the ICD.

Annex 2-D
Capability Development/Production Document (CDD/CPD) Content Guidance

See reference (e), enclosures F/G, appendix A, for mandatory CDD/CPD formats.

Reference (e), enclosures F/G, appendix A, **CDD/CPD format paragraphs/sections 6b, 6c, 10, 13, 14, and 15 and mandatory appendices**, will be implemented for Navy systems as amplified below in this annex.

6. System Capabilities Required for the Current Increment.

Identify....

a. System Attributes Description. Provide....

b. System Attributes Performance. Present....

(1) Base all performance thresholds on an analysis of mission demands and comparable fleet and commercial system experience. Per reference (e), thresholds and objectives shall be presented in output-oriented, measurable, and testable terms. The degree of specificity, in setting initial threshold and objective values, is to be tailored to the system and the acquisition phase.

c. Key Performance Parameters (KPPs) and Additional Performance Attributes. Each KPP will be addressed in this paragraph. System supportability and manpower are specifically described in paragraphs 6c(1) and 6c(2) below. Provide....

(1) System supportability shall be a performance parameter per reference (e) as described below:

(a) Mission Capable/Full Mission Capable (MC/FMC) rates, focused on primary mission areas may be used as supportability performance parameters in CDD/CPDs for aircraft or ship platforms.

(b) Materiel Availability shall be a mandatory supportability KPP per references (b) and (e).

(c) For legacy system modifications, supportability should be a performance parameter and Materiel Availability shall be a mandatory supportability KPP for only those subsystems being upgraded.

(2) Manpower may be a KPP for selected systems as jointly determined by the program sponsor and the Manpower Sponsor (CNO

(N1)). Program sponsors should assume a default consideration for a manpower KPP unless they obtain prior agreement with CNO (N1).

(3) Readiness thresholds, normally supportability performance parameters or KPPs, should account for all system downtime, including scheduled maintenance.

(4) Diagnostics effectiveness thresholds should be established for systems whose faults are to be detected by external support equipment or Built-In-Test (BIT). Threshold parameters should include percent correct fault detection and percent correct fault isolation to a specified ambiguity group. False alarm parameters should state thresholds in time (i.e. Mean Time Between False Alarms) or in percent.

(5) Materiel Reliability and Ownership Cost shall be mandatory Key System Attributes (KSAs) per references (b) and (e). Measures of operational system reliability should consist of both mission and logistics reliability parameters, as appropriate. Mean Time Between Operational Mission Failure (MTBOMF) should be used as the mission reliability parameter. Mean Time Between Failure (MTBF) should be used as the logistics reliability parameter. These parameters should be used as the operational system reliability parameters during OT&E, including Initial Operational Test and Evaluation (IOT&E) (OPEVAL).

10. Electromagnetic Environmental Effects (E3) and Spectrum Supportability

a. Establish E3 protection and spectrum supportability requirements for the following:

(1) Hazards of Electromagnetic Radiation to Ordnance (HERO)

(2) Hazards of Electromagnetic Radiation to Personnel (HERP)

(3) Hazards of Electromagnetic Radiation to Fuel (HERF)

(4) Electromagnetic Pulse (EMP)

(5) Electromagnetic Emission Control (EMCON)

(6) Electromagnetic Emissions Security (EMSEC)

(7) Electrostatic Discharge (ESD)

(8) Precipitation Static (P-Static)

(9) Lightning protection

(10) Range of frequency operations including within host, allied, and coalition nations

(11) Threat emitters

13. Other Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities (DOTMLPF) and Policy Considerations

a. HSI considerations that have a major impact on system effectiveness, suitability, and affordability should be addressed in section 13. The DOTMLPF implications, to include all the HSI domains, associated with deploying/fielding the system should be discussed in section 13 of the CDD and CPD. This section should provide a short description of the HSI issues and Fleet concerns regarding implementation of the materiel solution. This section should describe the safety and occupational health requirements, and environmental compliance expectations and associated costs.

14. Other System Attributes

a. Capabilities-oriented, performance-based HSI requirements that drive design, cost and/or risk should be included in section 14 of the CDD and CPD. HSI performance requirements should be specific and explicit in identifying the human performance contribution required to ensure total system performance and mission success. HSI performance requirements should optimize human-machine performance under operational conditions. HSI requirements should include thresholds and objectives and identify the Measures of Effectiveness (MOEs). Statements describing analyses that lead to specific human performance requirements should be avoided unless the level of fidelity of the Concept of Operations (CONOPS), program or technology is lacking. These analyses should be conducted as part of the requirements determination effort similar to any other system component. When fidelity is lacking, section 14 should contain broad constraints for the HSI requirements so that future revisions of the CDD will represent a refinement of the requirements and not the addition of new requirements.

HSI requirements should address, but are not limited to:

(1) Broad manpower constraints for the minimum number and appropriate mix (military, civilian and contractor) of operators, maintainers, trainers and support personnel.

(2) Manpower factors that impact system design (e.g., utilization rates, pilot-to-seat ratios, maintenance concepts).

(3) Identification of required Knowledge, Skills and Abilities (KSAs), aptitudes and physical characteristics of operators, maintainers and support personnel.

(4) Requirements for the training support package and logistics (e.g., technical documentation, simulators, training devices, new learning techniques, simulation technology, embedded training); requirements for individual, collective and joint training for operators, maintainers and support personnel.

(5) Human performance requirements that contribute to total system performance and mission success; the cognitive, sensory and physical requirements of the operators, maintainers and support personnel; ergonomic requirements for visual displays and their images, keyboards and other Input/Output (I/O) devices, workstations, and the operational environment; constraints or limitations on size or layout of system, equipment, and/or workspace.

(6) System safety and occupational health requirements that will eliminate reduce and mitigate the potential for injury, illness or disability and death of the operators, maintainers and support personnel.

(7) System requirements that reduce the risk of, prevent fratricide, and/or increase the odds of surviving fratricide, personal detection or targeting, or confinement within an attacked entity. Examples include egress from confined spaces, location of berthing and mess facilities within a ship or submarine, ejection seats and assisted breathing devices.

(8) Personnel support service requirements such as berthing and personal stowage, food service, medical, chapel and brig facilities, recreational and lounge spaces; ambient environment requirements (e.g., noise, lighting, Heating, Ventilation, and Air Conditioning (HVAC)).

b. As appropriate, address attributes that tend to be design, cost, and risk drivers, including Environmental, Safety, and Occupational Health (ESOH) quality; information protection standards for Intelligence, Surveillance, and Reconnaissance (ISR) platforms and other platforms as required; and Information Assurance (IA).

c. Address safety issues regarding Hazards of Electromagnetic Radiation to Ordnance (HERO).

d. Identify Extended Markup Language (XML) and any other system data standards, data accuracy, and data forecast required for net-centric data interoperability.

e. Identify weather, oceanographic, astrogeophysical, geospatial, and time support needs throughout the system’s expected life-cycle. Standard geospatial reference frame is defined by the World Geodetic System 1984 (WGS-84). Time, in terms of the standard temporal reference, is defined by Coordinated Universal Time (UTC) as maintained by the U.S. Naval Observatory (USNO) Master Clock, which is the standard for

military systems.

15. Program Affordability. The affordability ....

a. Operations and Support (O&S) Cost

Per reference (e), O&S shall be established as a cost parameter starting with the initial system CDD/CPD. Specifying O&S cost criteria with an associated threshold and objective places emphasis on optimizing the most significant portion of program cost. The methodology by which this parameter should be measured should be made clear by the requirements sponsor in the CDD/CPD, and involves concurrence with the testing community, cost estimators, and the system program office.

Mandatory Appendices

Appendix A. Architectural Products for Information Technology (IT) systems, including National Security Systems (NSS). Include only the required architecture framework view products developed from integrated architectures.

a. Mandatory (except as noted in footnotes 1, 2, and 3 and para b.)

Table E2T2 Net-Ready Key Performance Parameter Products Matrix (see Tables D-1, D-2, D-3, & D-4 CJCSI 6212.01D 8 Mar 06)

Document	Integrated Architecture Products (IAW DoDAF) [8]																NCOW RM [4]	KIP Compliance [5]	IA Compliance [6]
	AV-1	OV-1	OV-2	OV-3	OV-4	OV-5	OV-6C	OV-7	SV-1	SV-2	SV-4	SV-5	SV-6	SV-11	TV-1	TV-2			
JCD																			
ICD		x																	
CDD	x	x	x	x[1]	x	x	x	x[2]		x	x	x	x		x	x[2]	x	x	x
CPD	x	x	x	x[1]	x	x	x	x[2]		x	x	x	x	x[2]	x	x	x	x	x
ISP	x	x	x		x	x	x	x		x	x	x	x	x	x	x	x	x	x
TISP[7]	x	x[3]				x	x[3]		x[3]			x	x		X		x	x	x

1 = OV-3 (Operational Information Exchange matrix; see DoD Architecture Framework, ver 1.5, Vol I, 23 Apr 07 (definitions and guidelines)) is not assessed as part of the NR-KPP review; however, normally the OV-3 is used to develop other architecture documents and can be included with the NR-KPP documentation to assist in development and conduct of testing.
2 = OV-7 (Logical Data Model), SV-11 (Physical Schema), and TV-2 (Technical Standards Forecast) are required only when applicable.
3 = Tailored Information Support Plan (TISP) OV-1, OV-6C, and SV-1 may be waived by Joint Staff /J6-I.
4 = Net-Centric Operations and Warfare Reference Model (NCOW RM)
5 = Key Interface Profile (KIP)
6 = Information Assurance (IA)
7 = TISP for ACAT II, III, and IV programs
8 = Per CJCSM 3170.01C, the Joint Staff may waive the requirement for certain architecture views for CDDs and CPDs on a case-by-case basis based on the proposed joint potential designator (JPD) and presence or absence of a NR-KPP.

b. Per CJCSM 3170.01C: OV-7 and TV-2 as applicable for CDD/OV-7 and SV-11 when applicable for CPD

Appendix B. References

Appendix C. Acronym List

Annex 2-E
FORCEnet Consolidated Compliance Checklist for Development of IT, including National Security Systems (NSS), JCIDS Capabilities Documents and Acquisition Implementation

FORCEnet Consolidated Compliance Checklist (Example)					
		Meets	**Meets with Comment**	**Does Not Meet**	**Signature/ Date**
FORCEnet Operational Criteria	□ FORCEnet Integrated Architecture, Operational Views - Ref: CJCSI 3170.01F/CJCSM 3170.01C/CJCSI 6212.01D - Ref: DoD Architecture Framework (DoDAF) ver 1.5 of 23 Apr 07 DoDAF ver 1.5 - Volume I (definitions and guidelines) DoDAF ver 1.5 - Volume II (arch products description) DoDAF ver 1.5 - Volume III (arch data descriptions) - Ref: DOD Architecture Registry System (DARS) https://dars1.army.mil/ - Ref: SNI 5000.2D, basic 7b(1), 7c(1), 2.1, 2.1.2.5, 2.5.4.2, 5.4.7.1, 5.4.7.2, 5.4.7.10, 7.1.6.2, 7.1.6.3 - Ref: DON Acquisition and Capabilities Guidebook, Annex 2-D				
	□ FORCEnet Capabilities - Ref: CNO/CMC FORCEnet Functional Concept (7 Feb 05)				
FORCEnet System and Technical Criteria	□ FORCEnet Integrated Architecture, System and Technical Views - Ref: CJCSI 3170.01F/CJCSM 3170.01C/CJCSI 6212.01D - Ref: DoD Architecture Framework (DoDAF) ver 1.5 of 23 Apr 07 DoDAF ver 1.5 - Volume I (definitions and guidelines) DoDAF ver 1.5 - Volume II (arch products description) DoDAF ver 1.5 - Volume III (arch data descriptions) - Ref: DOD Architecture Registry System (DARS) https://dars1.army.mil/ - Ref: SNI 5000.2D, basic 7b(1), 7c(1), 2.1, 2.1.2.5, 2.5.4.2, 5.4.7.1, 5.4.7.2, 5.4.7.10, 7.1.6.2, 7.1.6.3 - Ref: DON Acquisition and Capabilities Guidebook, Annex 2-D				
	□ Naval Open Architecture Criteria as contained in the Open Architecture Assessment Tool (OAAT) - Ref: ASN(RD&A) memo of 5 Aug 04 - Ref: CNO(N6/N7) memo of 23 Dec 05 with Enclosure (1) - Ref: SNI 5000.2D, 3.4.6.1, 7.1.4				
	□ DoD Information Technology Standards Registry (DISR) https://disronline.disa.mil/a/DISR/index.jsp - Ref: CJCSI 6212.01D - Ref: OSD memorandum 20 Dec 04 https://disronline.disa.mil/a/DISR/index.jsp - Ref: DOD Architecture Registry System (DARS) https://dars1.army.mil/ - Ref: SNI 5000.2D, basic 7b(3), 7b(4), 7b(5), 7.1.6.2				
	□ Internet Protocol (IP) with transition to IPv6 planned - Ref: OSD memo 22 Aug 96 - Ref: DoD CIO memo 9 Jun 03 - IPv6 - Ref: ASD(NII) memo 16 Aug 05 - IPv6 Policy Update - Ref: DoD IPv6 Transition Plan Ver 2, 30 Jun 06 - Ref: DoD CIO memo 18 Jul 06 - IPv6 Implementation Schedules				
	□ Global Information Grid (GIG) Mission Area Capabilities - Ref: Initial Capabilities Document (ICD) for GIG Mission Area; - JROC memorandum 202-02 of 22 Nov 02 (updated 14 Aug 04)				

Annex 2-E (cont'd)
FORCEnet Consolidated Compliance Checklist for Development of IT, including National Security Systems (NSS), JCIDS Capabilities Documents and Acquisition Implementation

FORCEnet Consolidated Compliance Checklist (Example)					
		Meets	**Meets with Comment**	**Does Not Meet**	**Signature/ Date**
FORCEnet System and Technical Criteria	□ Global Information Grid (GIG) Enterprise Services (ES) - Ref: Initial Capabilities Document (ICD) for GIG ES 22 Mar 04 - Ref: JROCM 051-04 of 22 Mar 04 - Ref: SNI 5000.2D, basic ref (k)				
	□ Net-Centric Operations and Warfare Reference Model ver 1. 1 https://disain.disa.mil/ncow.html - Ref: CJCSI 6212.01D - Ref: SNI 5000.2D, 2.1.2.5 - Ref: DON Acquisition and Capabilities Guidebook, Annex 2-D				
	□ Net-Centric Enterprise Services (NCES) - Ref: DEPSECDEF memo GIG ES: Core Enterprise Services Implementation U18556-03 of 10 Nov 03 (see pg 2) - Ref: SNI 5000.2D, basic ref (k)				
	□ Net-Centric Enterprise Solutions for Interoperability (NESI) - Ref: Net-Centric Implementation Framework ver 1.3 http://nesipublic.spawar.navy.mil/				
	□ Net-Ready Key Performance Parameter (NR KPP) - Ref: CJCSI 3170.01F/CJCSM 3170.01C/CJCSI 6212.01D - Ref: DoD Architecture Framework (DoDAF) ver 1.5 of 23 Apr 07 DoDAF ver 1.5 - Volume I (definitions and guidelines) DoDAF ver 1.5 - Volume II (arch products description) DoDAF ver 1.5 - Volume III (arch data descriptions) - Ref: DOD Architecture Registry System (DARS) https://dars1.army.mil/ - Ref: SNI 5000.2D, 2.1.2.3, E3T4, 5.4.7.1 subpara 1, 5.4.7.2 subpara 4 - Ref: DON Acquisition and Capabilities Guidebook, Annex 2-D, 4.3, 4.4.2.1.2, 5.4.7.1 subpara 1, 5.4.7.2 subpara 4, 5.4.7.10.1.1				
	□ ASD(NII) Net-Centric Checklist (NCC) - Ref: OASD(NII) NCC ver 2.1.3 of 12 May 04 & 2.1.4 of 30 Jul 04 - Ref: DON Acquisition and Capabilities Guidebook, 4.4.1				
	□ Transformational Communications Architecture (TCA) - Ref: TCA ver 2.0 - Ref: DON Acquisition and Capabilities Guidebook, 7.1.6.2.1				
	□ Joint Tactical Radio System (JTRS) Software Compliant Architecture (SCA) - Ref: ASD(C3I) memoranda of 28 Aug 98 and 17 Jun 03 - Ref: DON Acquisition and Capabilities Guidebook, 7.1.6.2.2				
	□ Teleports - Ref: DoD Teleport Gen 2 ORD, 4 May 05 - Ref: DON Acquisition and Capabilities Guidebook, 7.1.6.2.3				
	□ Joint Battle Management Command and Control (JBMC2) Roadmap - Ref: JBMC2 Roadmap - Ref: DON Acquisition and Capabilities Guidebook, 7.1.6.2.4				

Annex 2-E (cont'd)
FORCEnet Consolidated Compliance Checklist for Development of IT, including National Security Systems (NSS), JCIDS Capabilities Documents and Acquisition Implementation

FORCEnet Consolidated Compliance Checklist (Example)					
		Meets	**Meets with Comment**	**Does Not Meet**	**Signature/ Date**
FORCEnet Policy Criteria	□ Human Systems Integration (HSI) - Ref: CJCSI 3170.01F/CJCSM 3170.01C, Encl F/G, App A, paras 13, 14 - Ref: SNI 5000.2D, basic 7k, 2.1.2.3, 2.4.6.1, 2.8.2, 3.4.7.1, 7.1, 7.2, 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.3 - Ref: DON Acquisition and Capabilities Guidebook, 7.2, Annex 2-C, paras 6a, 7b, 7c, Annex 2-D, paras 13a, 14a				
	□ Electromagnetic Environmental Effects (E3)/Spectrum Supportability (SS) - Ref: CJCSI 3170.01F/CJCSM 3170.01C, Encl F/G, App A, para 10 - Ref: CJCSI 6212.01D, Encl D - Ref: SNI 5000.2D, 2.4.6.1, E3T1, 3.7, E3T4, 7.1.13 - Ref: OPNAVINSTs 9070.1/3401.3 - Ref: DON Acquisition and Capabilities Guidebook, Annex 2-D, paras 10, 14c				
	□ Information Assurance (IA) - Ref: CJCSI 3170.01F/CJCSM 3170.01C, Encl F/G, App A, para 14 - Ref: CJCSI 6212.01D, SNI 5239.3A, OPNAVINST 5239.1B - Ref: SNI 5000.2D, basic 7c(6), 2.4.6.1, E3T1, 3.4.6.4, 4.2, 4.4, 5.4.7.11, 5.5.2, 5.7.4 - Ref: DON Acquisition and Capabilities Guidebook, Annex 2-D, para 14b				
	□ Data Strategy (DS) - Ref: CJCSI 3170.01F/CJCSM 3170.01C, Encl F/G, App A, para 14 - Ref: CJCSI 6212.01D - Ref: DoD Net-Centric Data Strategy, DoDCIO memo of 9 May 03 - Ref: SNI 5000.2D, 3.4.6.2, 4.3, 5.4.7.10, 7.1.6.1 SNI 5000.2D Chapters 2, 3, 4, 5, & 7 reference SNI 5000.36A - Ref: DON Acquisition and Capabilities Guidebook, Annex 2-D, para 14d				
	□ Geospatial, Time Standards, Meteorology, & Oceanography (GTSMO) - Ref: CJCSI 3170.01F/CJCSI 6212.01D/CJCSI 3901.01B - Ref: CJCSM 3170.01C, Encl F/G, App A, para 14 - Ref: SNI 5000.2D, 7.1.10, 7.1.11, 7.1.12, Ch 7 ref (t) is CJCSI 3901.01B - Ref: DON Acquisition and Capabilities Guidebook, Annex 2-D, para 14e				
Implementation Planning	□ CNO (N6/N7) Memo of 27 May 05, Subj: FORCEnet Requirements/Capabilities & Compliance Policy				
	□ ASN(RD&A) Memo of 14 Jul 05, Subj: DoN Acquisition Policy for Implementing FORCEnet Capabilities				

Annex 2-F
Weapon System and IT System Programs
ACAT Designation/Change Request (Content)

The memorandum requesting an Acquisition Category (ACAT) designation or requesting a change in ACAT designation should be sent to ASN(RD&A) for ACAT ID, IC, IAM, IAC, and II programs via the PEO/SYSCOM/DRPM, or to the cognizant PEO/SYSCOM/DRPM for weapon system or IT system ACAT III and ACAT IV programs, and should contain the following information:

1. Acquisition program short and long title.

2. Prospective claimant/SYSCOM/PEO/DRPM/PM.

3. Prospective funding: (where known)

   a. Appropriation (APPN): [repeat for each appropriation]

      (1) [Repeat for each program element (PE)/Line Item (LI)/Sub-project (Sub)]

      - Program Element (No./Title):
      - Project Number/Line Item (No./Title):
      - Sub-project/Line Item (No./Title):
      - Budget: [FY-2000 constant dollars in millions]

Current FY	Budget FY	FY	FY	FY	FY	FY	FY	To Complete	Total

4. Program description. (Provide a brief description of the program, including its mission.)

5. List Initial Capabilities Document, Capability Development/Production Document, and respective approval dates.

6. Program decision point status. (List completed milestones and dates; list scheduled program decision points and dates.)

7. Recommended ACAT assignment, or change, and rationale.

Copy to: ASN(RD&A) [ACAT III and IV programs]
ASN(RD&A)APA [all ACAT programs]
DASN(RD&A) [cognizant DASN for all ACAT programs]
CNO (N8/N091) [All Navy ACAT programs]
CMC (DC,CD&I) [All Marine Corps ACAT programs]
COMOPTEVFOR [All Navy ACAT programs]
Dir, MCOTEA [All Marine Corps ACAT programs]

Chapter 3
Statutory, Regulatory, and Contract Reporting Information and Milestone Requirements

References:
(a) DOD Directive 5000.1, The Defense Acquisition System, of 12 May 03
(b) DOD Instruction 5000.02, Operation of the Defense Acquisition System, of 8 Dec 08
(c) SECNAVINST 5200.38A
(d) Assistant Secretary of the Navy (Research, Development and Acquisition) Memorandum, DON Policy on Digital Product/Technical Data, of 23 Oct 04
(e) SECNAVINST 5000.36A
(f) SECNAVINST 5710.25B
(g) SECNAVINST 5510.34A
(h) SECNAVINST 4900.46B
(i) DOD Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), of 30 Jun 04
(j) CJCSI 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems, of 8 Mar 06
(k) DOD Directive 4650.1, Policy for Management and Use of the Electromagnetic Spectrum, of 8 Jun 04
(l) DOD Directive 3222.3, DoD Electromagnetic Environmental Effects (E3) Program, of 8 Sep 04
(m) DOD 5200.1-M, Acquisition Systems Protection Program, of 16 Mar 94
(n) DOD Instruction 5200.39, Critical Program Information (CPI) Protection Within the Department of Defense, of 16 Jul 08
(o) OPNAVINST 3432.1
(p) DOD Instruction S-5230.28, Low Observable (LO) /Counter Low Observable (CLO) Programs, of 2 Oct 00
(q) SECNAVINST 5239.3A
(r) OPNAVINST 5239.1B

3.1 Program Information

In support of SECNAV and ASN(RD&A), each Deputy Assistant Secretary of the Navy (DASN) for their cognizant ACAT I and II programs should review, provide input, and concur with appropriate acquisition related documents (e.g., Acquisition Program Baseline, Defense Acquisition Executive Summary, Selected Acquisition Report, Technology Development Strategy, Acquisition Strategy, Test and Evaluation Master Plan) prior to the documents being forwarded to ASN(RD&A) for concurrence or approval.

3.2 Exit Criteria

Exit criteria compliance should be reported in the Defense Acquisition Executive Summary (DAES) for ACAT I and IA programs.

3.3 Technology Maturity

Technology Readiness Levels (TRLs) listed in the Defense Acquisition Guidebook and in the Technology Readiness Assessment Deskbook may be used for assessing technology maturity in conducting technology readiness assessments (TRAs) for all ACAT programs. TRLs may be considered by the MDA in determining the maturity, risk, and readiness for transitioning new technologies into an ACAT program. Further guidance about technology transition is provided in the DUSD(S&T) document "Technology Transition for Affordability, A Guide for S&T Program Managers" of April 2001. This document can be accessed at https://www.dodmantech.com/pubs/TechTransGuide-Apr01.pdf .

Additionally, systems engineering technical reviews (for example the Alternative Systems Review and System Requirements Review) should be used to assess technology maturity in the context of system requirements, proposed program schedule, and independent estimate of program costs. These reviews can be a forum for subject matter experts to conduct Developing Activity (DA) independent technical assessments of technology maturity as it applies to the overall technical and programmatic approach.

The TRA Deskbook should be used as a guide for establishing independent TRA panels, identifying Critical Technology Elements (CTEs), planning and conducting TRAs, and developing Technology Maturation Plans (TMPs) for CTEs that require further maturation. The TRA Deskbook suggests timelines for events and methods for conducting and documenting TRAs. SYSCOMs should provide subject matter experts for membership on independent TRA panels, and whenever possible a standing SYSCOM TRA Expert Panel Chair, in support of Chief of Naval Research (CNR), PEOs, DRPMs, and PMs. CNR will provide direction for the conduct of Navy TRAs, and associated processes and outputs.

3.4 Technology Development and Acquisition Strategies

3.4.1 General Considerations for a Technology Development Strategy and an Acquisition Strategy

[***fm SNI 5000.2D, 3.4.1: PMs for all DON ACAT programs shall develop an acquisition strategy implementing a total systems engineering approach per references (a) and (b). For ACAT IC, IAC, and II programs, the PM shall develop the acquisition strategy in coordination with the Acquisition Coordination Team (ACT). The MDA shall approve a technology development strategy or an acquisition strategy, as appropriate, prior to the release of the formal solicitation for the respective phase.***]

Use of the discretionary procedures provided throughout this DON Acquisition and Capabilities Guidebook should assist PMs in developing acquisition strategies to execute ACAT programs that are well defined and carefully structured to represent a judicious balance of cost, schedule, performance, available technology, and affordability constraints prior to development, production, or deployment approval.

In developing an acquisition strategy, PMs should be aware that an evolutionary acquisition approach is the preferred strategy for rapid acquisition of mature technology for the user. An evolutionary approach delivers capability in increments, recognizing up front the need for future capability improvements. The process for implementing evolutionary acquisition, incremental development, is described in reference (b), enclosure 2, paragraph 2.

3.4.2 Requirements/Capability Needs

3.4.3 Program Structure

[***fm SNI 5000.2D, 3.4.3: Each acquisition strategy shall include a program structure, the purpose of which is to identify in a top-level schedule the major program elements such as program decision points, acquisition phases, test phases, contract awards, and delivery phases.***]

Each program structure should also include program elements that are necessary to execute a successful program, such as formal solicitation releases; systems engineering technical reviews including preliminary and critical design reviews; engineering development model, low-rate initial production, and full-rate production deliveries; developmental, live-fire, and operational test and evaluation phases; and initial and full operational capability dates. These program elements are contained in an acquisition strategy proposed by the PM and approved by the MDA. See references (a) and (b) and the Defense Acquisition Guidebook for direction and guidance on acquisition strategy program elements and implementation requirements for all DON ACAT programs.

3.4.4 Risk

[***fm SNI 5000.2D, 3.4.4: Plans for assessing and mitigating program risk shall be summarized in the acquisition strategy. PMs, utilizing SYSCOM engineering and logistics technical authority expertise, shall conduct a risk assessment identifying all technical, cost, schedule, and performance risks. In conjunction with the risk assessment, plans for mitigating those risks shall be conducted prior to each milestone decision and the Full-Rate Production Decision Review (FRP DR). PMs for all DON programs shall, for the purpose of reducing or mitigating program risk, research and apply applicable technical and management***

lessons-learned during system development, procurement, and modification.]

System engineering technical reviews should be used as an integrated technical risk assessment tool. Technical reviews (such as the System Requirements Review, Preliminary Design Review, Critical Design Review, System Verification Review, Production Readiness Review) conducted by independent subject matter experts with the program team can be an effective method of ascertaining technical risk at key points in the acquisition life cycle. Technical risks and associated mitigation approaches identified at these reviews should be incorporated into the program plan and budget.

ESOH and reliability should be considered in the overall program risk management process. Additional guidance on risk management and system safety implementation may be found in the Defense Acquisition Guidebook.

3.4.4.1 Interoperability and Integration Risk

[***fm SNI 5000.2D, 3.4.4.1, last subpara: For ACAT I, IA, and II programs and applicable ACAT III and IV programs that are designated by ASN(RD&A) for integration and interoperability special interest, risk assessment planning shall be coordinated with ASN(RD&A) Chief Systems Engineer (CHSENG) six months prior to program decision briefings. Developed risk assessments and mitigation plans for such programs shall be submitted to ASN(RD&A) CHSENG no later than 30 calendar days prior to program decision briefings. ASN(RD&A) CHSENG shall advise ASN(RD&A) and the PM of the adequacy of the integration and interoperability risk assessment and risk mitigation plan.***]

ASN(RD&A) CHSENG is available to assist the PM in the identification of integration and interoperability risks or in the use of interoperability and integration risk assessment tools. ASN(RD&A) publication NAVSO P-3686, "Top Eleven Ways to Manage Technical Risk," should be used as a guideline for establishing a technical risk management program. Several risk assessment tools are available in the Defense Acquisition Guidebook to assist in the identification of risks. Additionally, systems engineering technical reviews should be used as an integrated technical risk assessment tool.

3.4.5 Program Management

3.4.5.1 Integrated Digital Environment (IDE)

Engineering and logistics technical data for new systems, modeling and simulation, and applicable engineering and logistics technical data from legacy systems which interface with new systems; should be acquired and developed in digital electronic form to perform life-cycle support using digital operations per references (c), (d), and (e). The DON policy on digital logistics technical data, reference (d), provides guidance on acquisition and conversion of logistics technical data to digital form. See the Defense Acquisition Guidebook for implementation guidance for all DON programs.

3.4.5.2 Technical Representatives at Contractor Facilities

See the Defense Acquisition Guidebook for implementation guidance for all DON ACAT programs.

3.4.5.3 Government Property in the Possession of Contractors (GPPC)

PMs who have or use GPPC should have a process in place to ensure the continued management emphasis on reducing GPPC and the preventing of any unnecessary additions to GPPC. See the Defense Acquisition Guidebook for GPPC monitoring guidance for all DON programs.

3.4.5.4 Planning for Simulation-Based Acquisition (SBA) and Modeling and Simulation (M&S)

Reference (c) provides guidance for DON modeling and simulation management. See the Defense Acquisition Guidebook for implementation guidance for all DON ACAT programs.

3.4.6 Design Considerations Affecting the Acquisition Strategy

3.4.6.1 Open Architecture

3.4.6.2 Interoperability and Integration

[***fm SNI 5000.2D, 3.4.6.2: For programs that are part of a SoS or FoS, interoperability and integration shall be a major consideration during all program phases per reference (j). All programs shall implement data management and interoperability processes, procedures, and tools, per reference (e), as the foundation for information interoperability.***]

Interoperability and integration risks should be identified using the guidance in the Defense Acquisition Guidebook. Interoperability and integration include considerations such as physical/mechanical interchangeability and

"form, fit, and function," as well as the exchange of data and services.

3.4.6.2.1 Integrated Architecture

3.4.6.3 Aviation Critical Safety Items

Aviation critical safety items (CSIs) are parts, assemblies, installations, launching or recovery equipment, or support equipment containing a critical characteristic whose failure, malfunction, or absence may cause a catastrophic or critical failure resulting in loss or serious damage to the aircraft or weapon system, unacceptable risk of personal injury or loss of life, or an uncommanded engine shutdown resulting in an unsafe condition.

3.4.6.4 Information Assurance

[***fm SNI 5000.2D, para 3.4.6.4: Information assurance (IA) requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, and replacement of all DON information systems per 10 USC 2224, Office of Management and Budget Circular A-130, and reference (b). PMs shall develop an IA Strategy and summarize the IA Strategy in the program's overall acquisition strategy.***]

PMs should ensure the acquisition strategy provides for compliance with the procedures regarding IA. PMs should summarize in the acquisition strategy the technical, schedule, cost, and funding issues associated with executing requirements for IA, and maintain a plan to resolve any issues that arise. This effort should ensure that IA policies and considerations are addressed and documented as an integral part of the program's overall acquisition strategy. The IA strategy should define the planning approach the PM will take during the program to ensure that IA requirements are addressed early on and Clinger-Cohen Act requirements for IA are captured as part of the program's overall acquisition strategy. The IA strategy will continue to evolve during development through test and evaluation, so that by Milestone C it contains sufficient detail to define how the program will address the fielding and support requirements that meet material readiness and performance objectives.

3.4.6.5 Standardization and Commonality

3.4.6.6 Protection of Critical Program Information and Anti-Tamper (AT) Measures

See this Guidebook, paragraphs 3.8.1 and 3.8.1.1 for AT guidance.

3.4.7 Support Strategy

[***fm SNI 5000.2D, 3.4.7: Support planning shall show a balance between program resources and schedule so that systems are acquired, designed, and introduced efficiently to meet CDD/CPD and APB performance design criteria thresholds. The PM as the life-cycle manager, designated under the tenets of Total Life Cycle Systems Management (TLCSM), shall document the product support strategy in the acquisition strategy. Performance Based Logistics (PBL) is the preferred support strategy and method of providing weapon system logistics support. A comprehensive business case analysis will be the basis for selecting a support strategy and reflecting the associated tradeoffs (e.g., between performance, technical, business, organic/commercial considerations). A program level PBL implementation plan shall be developed for all programs using a PBL support strategy.***]

Support planning, and its execution, forms the basis for fleet or Marine Corps forces introduction and deployment recommendations and decisions. Reliability, availability, and maintainability are critical considerations in the development of the support strategy. See the Defense Acquisition Guidebook for implementation guidance for all DON ACAT programs.

The PM, in coordination with military service logistics commands, is the Total Life-Cycle Manager (TLCM). This includes full life-cycle product support execution and resource planning responsibilities. The overall product support strategy, documented in the acquisition strategy, should include life-cycle support planning and should address actions to assure sustainment and to continually improve product affordability for programs in initial procurement, re-procurement, and post-production support.

3.4.7.1 Human Systems Integration (HSI)

[***fm SNI 5000.2D, 3.4.7.1: The acquisition strategy shall summarize HSI planning, including how the program will meet HSI programmatic requirements and standards. It shall describe how the system will meet the needs of the human operators, maintainers, and support personnel. This includes Manpower, Personnel, and Training (MPT), human factors engineering, personnel survivability, and habitability, safety, occupational health, and environmental considerations.***]

The summary of HSI planning included in an acquisition strategy should illustrate how the PM intends to effectively meet the HSI requirements in the DOD 5000 series and SECNAVINST 5000.2D. The Navy’s established Enterprise approach to HSI is called Systems Engineering, Acquisition and Personnel Integration (SEAPRINT).

The following information should be considered in

developing the HSI section of an acquisition strategy. However, if the MDA and the PM elect to require a separate HSI Plan (see paragraph 3.9.1 of this guidebook), this information should be included in that document; the acquisition strategy can then refer to the HSI Plan.

1. Provide a summary overview of the HSI strategy, addressing HSI risk assessment and reduction, application of technology in the achievement of HSI objectives, establishment of HSI priorities, and a description of the process to be implemented to ensure HSI objectives are met.

2. Explain, with rationale, any tailoring of required HSI activities.

3. Provide a complete list of all commands and activities involved with the HSI effort; explain the organizational structure of the program (including industry partners) and describe the role of the HSI team within that structure.

4. Describe how HSI will be integrated with all acquisition logistics support (ALS) analyses and activities.

5. Summarize HSI constraints and results of the HSI analyses and trade-offs.

6. Describe prior decisions, assumptions, mandated constraints and information pertaining to HSI.

7. Describe the total systems approach (hardware, software, human); describe how the performance characteristics for humans were integrated into the system.

8. Develop a tailored list of all HSI activities by milestone; show the POA&M for HSI activities overlaid with the program schedule; highlight any inconsistencies or conflicts.

9. Describe how HSI requirements contribute to mission capability, material readiness, force structure, affordability, performance effectiveness, and achievement of wartime operational objectives.

10. Describe the total system performance goals that require HSI-related design interface and support analysis.

11. Identify key issues that have HSI implications, including constraints established in the Initial Capabilities Document (ICD); include major design, material readiness, test and evaluation, and affordability issues.

12. Summarize how the system addresses the cognitive, sensory, and physical needs of the human operators. Summarize the approach for human-centered design initiatives.

13. Identify the HSI analyses to be conducted and their effects on managing HSI risks.

3.4.7.2 Environmental, Safety, and Occupational Health (ESOH) Considerations

3.4.7.3 Demilitarization and Disposal Planning

3.4.7.4 Post Deployment Performance Review

[***fm SNI 5000.2D, 3.4.7.4: The acquisition strategy shall address the statutory requirement for a post deployment performance review for ACAT I and IA programs.***]

The primary focus of post deployment performance reviews (PDPRs) is on how well an ACAT I or IA program is meeting its mission, performance, management, financial, and technical goals. Senior management for ACAT IA programs will review the PDPR reports for inputs to IT investment decisions. Guidance to assist organizations in conducting PDPRs of IT investments as required by the Clinger-Cohen Act of 1996 is provided in the DON IT Investment Evaluation Handbook, which can be found on the DON Chief Information Officer (CIO) website at http://www.doncio.navy.mil/Products.aspx?ID=757. PDPRs should consider safety and survivability as well as the effectiveness of the implementation of human systems integration strategies. See the Defense Acquisition Guidebook for PDPR implementation guidance for all applicable programs.

3.4.7.5 Program Protection Planning

3.4.7.6 Product Support

3.4.7.6.1 Product Support Management Planning

Planning for a performance based logistics (PBL) strategy should be rationalized by support analysis, baseline assessment, and the establishment of support performance metrics. PBL decisions should also be based on the operational environment and the logistics infrastructure’s ability to support non-PBL defense programs. PBL requirements should be invoked with contractors where appropriate. A guide for the development of a PBL strategy for product support of weapon systems titled "A Program Manager’s Guide to Buying Performance" is available on the ASN(RD&A) web page which can be found at http://www.acquisition.navy.mil/.

3.4.7.7 Planning for Parts and Materials Obsolescence

Support planning should include a process to resolve problems created by parts and/or materials obsolescence and reduce or eliminate any negative impacts. Such planning should proactively consider the impact of obsolescence on the acquisition life cycle by anticipating potential obsolescence and taking appropriate logistics, acquisition, and budgeting steps to prevent obsolescence from adversely affecting material readiness or total ownership cost. As a necessary adjunct to this element of support planning, the process should ensure that obsolescence mitigation information is effectively communicated and exchanged within DON, with other Government organizations, and with industry through maximum use of alerts and the Government-Industry Data Exchange Program (GIDEP).

3.4.8 Business Strategy

3.4.8.1 International Cooperation*

[***fm SNI 5000.2D, 3.4.8.1: PMs for DON ACAT programs shall consult with the Navy International Programs Office (IPO) during development of the international element of the program's acquisition strategy to obtain:***

1. Relevant international programs information,] such as research, development, and acquisition international agreements that are existing, proposed, or under consideration by allies and friendly nations; anti-tamper policies; and data exchange agreements with allied and friendly nations.

2. [***fm SNI 5000.2D, 3.4.8.1: ASN(RD&A) policy and procedures regarding development, review, and approval of international armaments cooperation programs,***] as established by reference (f).

3. [***fm SNI 5000.2D, 3.4.8.1: DON technology transfer policy***] established by references (g) and (h) under the policies of the Secretary of Defense as recommended by the National Disclosure Policy Committee (NDPC).

See the Defense Acquisition Guidebook for implementation guidance for all DON ACAT programs.

*This paragraph is not normally applicable to IT programs.

3.4.8.1.1 International Cooperative Strategy

The business strategy should identify similar programs/projects under development or in production by an ally. The acquisition strategy assesses whether a similar program/project could satisfy U.S. requirements, and if so,

recommend designating the program an international cooperative program. DON PMs and/or PEOs should consult with the Navy IPO in order to ensure their programs are consistent with Navy International Programs Office campaign plans for sales to allied and friendly nations.

3.4.8.1.2 International Interoperability

3.4.8.2 Competition

PMs should consider acquiring necessary rights in technical data and computer software sufficient to permit competing follow-on acquisitions.

3.4.8.3 Warranties

The PM should examine the value of warranties and pursue such warranties when appropriate and cost-effective. When appropriate, the PM should incorporate warranty requirements in the contractual language per Federal Acquisition Regulation Subpart 46.7 and Defense Federal Acquisition Regulation Supplement paragraph 246.7. See the Defense Acquisition Guidebook for implementation guidance for all DON ACAT programs.

3.5 Intelligence Support

3.6 Command, Control, Communications, Computers, and Intelligence (C4I)/Information Support

[***fm SNI 5000.2D, 3.6: PMs shall develop Information Support Plans (ISPs) (formerly the C4I Support Plans (C4ISPs)) for those IT, including NSS, ACAT programs that connect in any way to the communications and information infrastructure. ISPs are to be developed per the requirements in reference (b).***]

See the Defense Acquisition Guidebook for C4I/Information Support Plan implementation guidance and formats for IT, including NSS, ACAT I, IA, II, III, and IV programs when they connect in any way to the communications and information infrastructure.

C4ISPs/ISPs for IT, including NSS, ACAT I and IA programs, and Assistant Secretary of Defense (Networks and Information Integration) (ASD(NII)) special interest IT, including NSS, programs are to be entered into the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) for review. After approval, C4ISPs/ISPs for all IT, including NSS, programs are to be entered into the JCPAT-E repository for retention per references (i) and (j).

3.7 Electromagnetic Environmental Effects (E3) and Electromagnetic Spectrum Certification and Supportability

E3 control is concerned with design and engineering to minimize the impact of the electromagnetic environment on equipment, systems, and platforms. E3 control applies to the electromagnetic interactions of both spectrum-dependent and non-spectrum-dependent objects within the operational environment. Examples of non-spectrum-dependent objects that could be affected by the electromagnetic environment are ordnance, personnel, and fuels. The increased dependency on and competition for portions of the electromagnetic spectrum have amplified the likelihood of adverse interactions among sensors, networks, communications, and weapon systems.

The objective of establishing E3 control requirements in the acquisition process is to ensure that DON equipment, subsystems, and systems are designed to be self-compatible and operate compatibly in the operational electromagnetic environment. To be effective, the program manager should establish E3 control requirements early in the acquisition process to ensure compatibility with co-located equipment, subsystems, and systems, and with the applicable external electromagnetic environment.

National, international, and DoD policies and procedures for the management and use of the electromagnetic spectrum require program managers developing spectrum-dependent systems/equipment to consider spectrum supportability requirements and E3 control early in the development process. Given the complex environment (both physical and political) in which DoD forces operate, and the potential for worldwide use of capabilities procured for DoD, early and thorough consideration is vitally important. The spectrum supportability process includes the following:

1. The spectrum-dependent system/equipment being acquired is designed to operate within the proper portion of the electromagnetic spectrum;

2. Permission has been (or can be) obtained from designated authorities of sovereign ("host") nations (including the United States and Protectorates) to use that equipment within their respective borders; and

3. The newly acquired equipment can operate compatibly with other spectrum dependent equipment already in the intended operational environment (electromagnetic compatibility).

References (k) and (l) implement E3 and spectrum management/spectrum certification within the Navy and Marine Corps, respectively. See reference (b), enclosure 4, for implementation requirements for all DON ACAT programs. Expanded

guidance is available from the Defense Acquisition Guidebook.

3.7.1 Electromagnetic Environmental Effects (E3)

Achievement of compatibility in the operational electromagnetic environment is the paramount objective of the Navy E3 Program. The Navy E3 program's primary goal is to enhance force performance by institutionalizing the prediction and design of the operational Navy electromagnetic environment (EME), and the correction, prevention, and control of degradation to warfighting capability caused by the interaction of the EME with Navy equipment, systems, platforms, and personnel. E3 design requirements for all DON communications and electronics (C-E) systems and equipment should be identified in all necessary acquisition documents during the DON acquisition process and integrated into all developmental and operational tests per references (k) and (l). E3 design requirements should apply to all phases of the acquisition process and should be implemented as early as possible in the conceptual, design, acquisition, and operational phases of all equipment, systems and platforms. E3 control should be planned for and incorporated in all Navy equipment, systems and platforms including commercial items and non-developmental items.

All munitions and electric or electronic systems and equipment will be designed or procured to be mutually compatible with other electrical or electronic equipment within their expected operational environment. This encompasses electromagnetic compatibility (EMC)/electromagnetic interference (EMI); electromagnetic vulnerability (EMV); electromagnetic pulse (EMP); electrostatic discharge (ESD); hazards of electromagnetic radiation to personnel (HERP), to ordnance (HERO), and to fuel (volatile materials) (HERF); and natural phenomena effects of lightning and precipitation static (P-static).

Key Review Actions by Program Managers:

1. Define, and update as necessary, applicable electromagnetic environments where systems/equipment are/is intended to operate;

2. Establish E3 control requirements, with special emphasis on mutual compatibility and HERO guidance;

3. Define E3 programmatic requirements to include analyses, modeling and simulation, and test and evaluation; and

4. Ensure that E3 developmental test and evaluation/ operational test and evaluation requirements and spectrum management planning and analyses are addressed in the Test and Evaluation Master Plan, and that resources are identified to support these activities.

3.7.2 Electromagnetic Spectrum Certification and Supportability

Spectrum certification effects spectrum supportability. The program manager should initiate the spectrum certification (DD Form 1494 Application for Equipment Frequency Allocation) process prior to Milestone B to ensure spectrum supportability early in the development cycle.

Spectrum certification is the statement of adequacy received from authorities of sovereign nations after their review of the technical characteristics of spectrum dependent equipment or systems regarding compliance with their national spectrum management policy, allocations, regulations, and technical standards. The purpose of spectrum certification is to:

1. Obtain authorization from the National Telecommunications and Information Administration to develop or procure items that use a defined frequency band(s) or specified frequencies to accommodate a specific electronic function(s);

2. Ensure compliance with national policies and allocation tables which provide order in the use of the radio frequency spectrum; and

3. Ensure spectrum availability to support the item in its intended operational environment.

The spectrum certification process is used to receive an approved electromagnetic frequency allocation and Host Nation Agreement if the system is to operate in international electromagnetic environments. A DD Form 1494, Application for Equipment Frequency Allocation, is required for spectrum certification by the Military Communications-Electronics Board (MCEB) for all spectrum dependent systems and all systems employing satellite techniques (47 U.S.C. Sections 901-904). Spectrum dependent systems are those electronic systems, subsystems, and devices and/or equipment that depend on the use of the electromagnetic spectrum for the acquisition or acceptance, processing, storage, display, analysis, protection, disposition, and transfer of information.

1. The DD Form 1494 documents the spectrum-related technical and performance characteristics of an acquisition item to ensure compliance with the applicable DoD, individual national, both U.S. and foreign, and international spectrum management policies and regulations.

2. The DD Form 1494 is routed through command channels to the sponsoring Military Department Frequency Management Office: the U.S. Army Spectrum Management Office, the Navy-Marine Corps Spectrum Center, or the Air Force Frequency Management Agency.

a. The Military Department representative then submits the form to the Spectrum Planning Subcommittee of the Interdepartmental Radio Advisory Committee under the National Telecommunications and Information Administration; and

b. The Service Frequency Management Office (FMO) submits the form to the Equipment Spectrum Guidance Permanent Working Group (ESG PWG) under the Frequency Panel of the Joint Staff MCEB.

Requirements for foreign spectrum support will be forwarded to the MCEB ESG PWG for coordination with host nations where deployment of the system or equipment is anticipated. Spectrum certification updates should be prepared at each subsequent acquisition milestone. The Navy and Marine Corps Spectrum Center can assist PMs with the spectrum certification process.

3.7.2.1 Electromagnetic Spectrum Certification Compliance

As part of the milestone review process, the MDA should ensure that electromagnetic spectrum supportability has been approved. Additionally, PMs should complete spectrum supportability assessment factors shown in Table E3T4 of enclosure (3) of SECNAVINST 5000.2D prior to award of a contract for acquisition of any system that employs the electromagnetic spectrum. The applicable program information shown in Table E3T4 are examples of the most likely references for the required information. If the PM deems other references more appropriate, they may be used in addition to or instead of those cited.

3.7.2.2 Electromagnetic Spectrum Supportability

3.8 Technology Protection

[***fm SNI 5000.2D, 3.8: Each DON program that contains critical program information or critical technology shall prepare a Program Protection Plan (PPP) per references (m) and (n). PPPs shall include a PM-approved classified Anti-Tamper (AT) Annex that has Naval Air Systems Command (NAVAIRSYSCOM)'s technical concurrence as DON's AT Technical Authority. ASN(RD&A) CHSENG is the DON point-of-contact for DoD and DON AT policy matters and for working with the DoD AT Executive Agent.***

CNO (N2, N3/N5, and N6) shall provide operations security (OPSEC) and OPSEC enhancement planning guidance during ICD review. CNO (N2, N3/N5, and N6) shall coordinate guidance preparation and shall assist the PM's staff in subsequent OPSEC and program protection planning involving critical program information. Detailed policy and procedures are found in reference (o).]

The PPP should encompass security, acquisition systems protection, systems security engineering, counterintelligence, and operations security (SASCO) requirements. SASCO requirements are contained in reference (n). A discretionary, illustrative format for a PPP is provided in reference (m). See reference (b), enclosure 4, for implementation requirements for all DON ACAT programs.

3.8.1 Anti-Tamper Measures

Technology protection is essential to maintain technological superiority over a system's life. Additionally, DoD seeks to cooperatively develop systems with other countries and permit Foreign Military Sales (FMS) or Direct Commercial Sales (DCS), which promote resource conservation, standardization, commonality, and interoperability. Co-development, sales, transfer loss on the battlefield, and/or unintended diversion will expose critical technology to potential exploitation or reverse-engineering attempts. This unintentional technology transfer risk must be addressed by assessing, designing, and implementing appropriate AT measures.

DON's AT Technical Agent (Office of Naval Research (ONR)) will support PMs and DON's AT Technical Authority (NAVAIRSYSCOM) on AT technical matters.

3.8.1.1 Program Protection Plan AT Annex

ACAT programs that contain critical program information are required by reference (b) to develop a Program Protection Plan with an AT Annex. The DON AT technical agent will be available to assist the PM in preparing and staffing the AT Annex. A final Program Protection Plan AT Annex will be submitted to ASN(RD&A) CHSENG via the DON AT technical agent for AT Annex technical concurrence at least 60 days prior to any program decision point (i.e., milestone, FMS decision date, etc). Effective AT Annex development should include the following:

1. Identify critical program information and technologies per references (n), (o), (p), (q), (r), and the Militarily Critical Technologies List (http://www.dhra.mil/perserec/csg/t1threat/mctl.htm).

2. Assess the vulnerabilities and risk of inadvertent technology transfer over the planned service life. FMS and DCS should be assumed for most programs unless compelling evidence exists to the contrary.

3. Identify potential technical solutions, determine likely cost and schedule implications, and select methods best suited to the respective acquisition effort. Early liaison with the DON AT Technical Agent can assist in effective technical solution selection. The cost must be identified and resourced by

the OPNAV Sponsor early in the program's life cycle.

4. Develop and resource the validation & verification of the planned AT implementation.

ASN(RD&A) CHSENG should be consulted for any revised DoD AT Executive Agent directed AT policy and guidelines which might impact an acquisition program.

3.9 Periodic Reporting

3.9.1 Program Plans

The below discussion of specific program plans does not imply that the plans addressed here constitute all of the planning documents that are or may be required of a specific program.

If international access, participation, or sales is planned or anticipated, the Program Protection Plan will include as annexes a Technology Assessment and Control Plan (TA/CP) (approved by the MDA) and a delegation of disclosure authority letter (DDL) (approved by ASN(RD&A) or formally delegated disclosure authority).

A Logistics Supportability Plan is a discretionary acquisition phase program plan that may be required by the MDA or PM. The Logistics Supportability Plan was formerly known as the Integrated Logistics Support Plan or Acquisition Logistics Support Plan. The Logistics Supportability Plan may be initially developed as early as program initiation and may be updated annually, until sustainment, to ensure life-cycle logistics management planning efforts are current and in coordination with program efforts.

A Systems Engineering Plan (SEP) is a mandatory milestone document that is required at Milestones A, B, and C and also program initiation for ships. The SEP may be an annex to the acquisition strategy or it may be a stand-alone document and summarized in the acquisition strategy. The SEP should detail the overall systems engineering process and effort to be used, how that process supports the assessment of technical health and technical baseline management, how technical reviews will be used to support program decisions, and how the systems engineering effort relates to other program activities and plans.

Preparation of a HSI Plan (HSIP) to document the process for effective planning and implementation of HSI activities is discretionary and may be required by the MDA or PM. An HSIP would assist in summarizing HSI planning for the acquisition strategy. PMs should prepare an HSIP before, or as soon as possible after, program initiation. An HSIP facilitates the integration of the HSI domains among themselves and between the HSI team and all stakeholders. The HSIP should include an HSI

issues audit trail that identifies and describes issues or concerns; plans to address each issue/concern; actions taken or decisions made; tradeoff decisions/reasons when costs or other constraints prohibit adoption of optimal HSI solutions or impact on performance and/or risk mitigation strategies; those responsible for action taken or decisions made; and the current status of each issue/concern. The HSIP should be a living document that is updated as the program evolves.

Preparation of a System Safety Program Plan (SSPP) is discretionary and may be required by the MDA or PM. A SSPP describes the tasks and activities required to implement the system safety program and includes organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort and integration with other program engineering and management activities and related systems. PMs who develop an HSIP are encouraged to integrate the SSPP and the HSIP into a single document or a single addendum to the acquisition strategy.

3.9.2 Acquisition Program Baseline (APB) Reporting

The PM reports the current estimate of each APB parameter periodically to the MDA. The PM reports the current APB estimates for ACAT I and IA programs quarterly in the DAES. Program goals of those programs that are part of a system of systems (SoS) or family of systems (FoS) will be established in the context of an individual system executing one, or more, mission capabilities of the SoS or FoS.

See the Defense Acquisition Guidebook and Annex 3-A of this enclosure for APB implementing guidance for all DON ACAT programs.

3.9.3 Defense Acquisition Executive Summary (DAES) -- (DD-AT&L(Q)1429)

[***fm SNI 5000.2D, 3.9.3: DAES monthly charts and information are required for ACAT I and IA programs. The DAES monthly charts shall be submitted to ASN(RD&A) no later than the 20th of each month, and the quarterly information shall be inputted into Dashboard for ASN(RD&A) review no later than the 20th day of the program's designated quarterly reporting month. Data will be electronically provided from Dashboard to USD(AT&L)'s Defense Acquisition Management Information Retrieval (DAMIR) System by the 28th of each month.***]

Reference (b), enclosure 4, requires ACAT I/IA DAES reporting which shall be in the consolidated acquisition reporting system (CARS) format (see the Defense Acquisition Guidebook).

3.9.3.1 DAES Reporting

Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) assigns DAES reporting responsibility. Selected ACAT I/IA programs are assigned a designated reporting month by USD(AT&L) to begin their quarterly DAES reports. DAES data will be electronically provided from Dashboard to USD(AT&L)'s Defense Acquisition Management Information Retrieval (DAMIR) System by the 28th of the program's designated quarterly reporting month. To meet this deadline and to allow adequate time for ASN(RD&A) and ASN (Financial Management and Comptroller) (ASN(FM&C)) review, DAES monthly charts are to be submitted to ASN(RD&A) no later than the 20th of each month, and the quarterly information shall be inputted into Dashboard for ASN(RD&A) review no later than the 20th day of the program's designated quarterly reporting month.

3.9.4 Selected Acquisition Report (SAR) -- (DD-AT&L(Q&A)823)*

[**fm** ***SNI 5000.2D, 3.9.4: The Secretary of Defense is required to submit to Congress an SAR for each ACAT I MDAP. Waivers may be granted by the USD(AT&L) for certain pre-Milestone B programs that do not have an approved Acquisition Program Baseline. The SAR provides to Congress standard, comprehensive summary reporting of cost, schedule, and performance information on each ACAT I program. The annual SAR report, covering the period ending 31 December, shall be submitted to ASN(RD&A) no later than the 15th day after the President sends the budget to Congress.***

Quarterly SARs, which are submitted on an exception basis, shall be forwarded no later than the 15th day after the end of the reporting quarter. Exception SAR reporting is required for programs when: 1) the current estimate exceeds the APB objective for the Program Acquisition Unit Cost or the Average Procurement Unit Cost by 15 percent or more; 2) the current estimate includes a six-month or greater delay, for any APB schedule parameter, that has occurred since the current estimate reported in the previous SAR; or 3) Milestone B or Milestone C approval occurs within the reportable quarter.]

SAR preparation implementation guidance for ACAT I programs is provided in the Defense Acquisition Guidebook.

*The SAR is not applicable to ACAT IA programs.

3.9.5 Unit Cost Reports (UCRs) –- (DD-AT&L(Q&AR)1591)*

*UCRs are not applicable to ACAT IA programs.

3.9.6 Past Performance Reporting/Reports

The DON automated system for reporting contractor past performance is the Contractor Performance Assessment Reporting System (CPARS) which is accessible via the Internet at http://www.cpars.csd.disa.mil/. PM's have the responsibility for providing an annual assessment of their contractors' performance via the CPARS.

3.9.7 Consolidated Acquisition Reporting System (CARS)

See the Defense Acquisition Guidebook for CARS implementation guidance for SARs for ACAT I programs and Acquisition Program Baselines for all ACAT programs.

3.10 Program Certification and Assessments

3.10.1 Certification Requirements at Milestone A

3.10.2 Certification Requirements at Milestone B

3.10.3 Assessments Required Prior to Approving the Start of Construction on First Ship of Shipbuilding Program

Annex 3-A
Weapon System and IT System Programs Acquisition Program Baselines (APBs)/ APB Deviations

1.1 Acquisition Program Baseline (APB)

Per references (a) and (b), every ACAT program shall establish an Acquisition Program Baseline (APB) that documents the cost, schedule, and performance objectives and thresholds of that program. The initial APB will be prepared in connection with the program's initiation, and will be maintained and updated as necessary per below guidance until the program is no longer on the active ACAT program list.

1.1.1 Objectives and Thresholds

Per reference (b), each parameter shall include both an objective and threshold value. If no threshold is specified, then the threshold value will be considered the same as the objective value. The APB will incorporate all of the parameters objectives and thresholds specified in the capabilities document (e.g., the Capability Development Document (CDD) or the Capability Production Document (CPD)). PMs for DON ACAT programs may propose additional program parameters, with associated objectives and thresholds, for approval by the milestone decision authority (MDA). Program objectives and thresholds must be quantifiable and measurable.

PMs will not make trade-offs in cost, schedule, and/or performance outside of the trade space between objective and threshold values without first obtaining approval from the appropriate requirements/functional and resource sponsors, and from the MDA.

For those programs that are part of a SoS or FoS, objectives and thresholds are to be established per the SoS or FoS Capstone Requirements Document (CRD).

1.1.2 APB Content

The APB content for all ACAT DON programs, including those APBs revised as a result of program modifications, will represent the program as it is expected to be developed, produced, and deployed.

1.1.2.1 Performance Parameters

The total number of performance parameters should be the minimum number needed to characterize the major drivers of operational performance, supportability, and interoperability. The minimum number includes the KPPs identified in the CDD or the CPD.

1.1.2.2 Schedule Parameters

Schedule parameters should minimally include dates for program initiation, major decision points, and the attainment of initial operating capability (IOC).

The threshold value for a weapon system APB schedule parameter should normally be the objective value plus six months.

1.1.2.3 Cost Parameters

The APB cost section of all DON weapon system programs, regardless of ACAT, should reflect the same parameters as those used in the format of the consolidated acquisition reporting system (CARS) generated APB for ACAT I programs. All cost parameter objectives and thresholds established in an APB should be stated in constant base year dollars, with the base year clearly identified. The weapons systems APB cost parameters should include: 1) the total cost for each separate cost parameter (RDT&E, procurement, military construction (MILCON), acquisition operations and maintenance (O&M), and operating and support (O&S)); 2) total quantity (including both fully-configured development and production units); 3) average procurement unit cost (defined as the total procurement cost divided by total procurement quantity); 4) program acquisition unit cost (defined as the total of all acquisition related appropriations divided by the total quantity of fully configured end items (including engineering development models (EDMs))); and 5) the total costs of any other cost objective(s) designated by the MDA. In addition, weapon systems APBs should include a total ownership cost (TOC) parameter consisting of direct costs (RDT&E, procurement, MILCON, acquisition items procured with operations and maintenance funds, and operations and support), indirect costs (attributable to the program’s system), and infrastructure costs (not attributable to the program’s system) for the life of the program. TOC and quantity amount parameters do not require a threshold as they are not breachable parameters.

Cost figures for all APBs should reflect realistic estimates to achieve performance objectives of the total program, including a thorough assessment of risk. Baseline costs should include the total program, not just the amount funded in the budget and programmed through the future years defense program (FYDP) (i.e., baseline costs should include

out-year (beyond the FYDP) funding requirements that are part of the approved program). Budgeted amounts should not exceed the total cost thresholds in the APB.

The threshold values for the cost parameters should normally be the objective value plus 10 percent.

1.1.3 Evolutionary Acquisition

When delivering systems under an evolutionary acquisition strategy, the APB will include parameters for the next increment and, if known, for follow-on increments. These follow-on increments should be established as a separate end item within the APB, where logical and feasible. Objectives and thresholds for cost, schedule, and performance will be included within the APB for each block/increment, in the level of detail available at the time.

When determining whether an effort should be considered an evolutionary acquisition, the question to be answered is whether the new effort is of an evolutionary or "revolutionary" nature. If the new effort is a drastic change or improvement that is "revolutionary" (as opposed to evolutionary) to the performance of the older effort, then the new effort must be considered as a separate and distinct new ACAT program and not simply a separate increment/end item within the existing ACAT program and APB.

1.2 Procedures

1.2.1 Preparation and Approval

All ACAT program APBs will be prepared by the PM and approved by the MDA as part of the mandatory program decision point information provided at program decision point meetings.

Once the revised APB has been approved by the MDA, the funding associated with the revised APB is to be reflected in the next FYDP update and is to be the new program funding.

IT program APBs will be prepared by the PM in coordination with the user or user’s representative.

1.2.1.1 ACAT I, IA, and II Endorsements

All APBs for ACAT I, IA, and II programs will be endorsed by the Program Executive Officer (PEO), Systems Command (SYSCOM) Commander, or Direct Reporting Program Manager (DRPM) (as appropriate).

Once the APB has been endorsed by the PEO, SYSCOM, or DRPM, it will be forwarded concurrently to the following organizations for endorsement:

1. CNO (Communication Networks (N6), or Fleet Readiness and Logistics (N4), (as appropriate)), and

2. CNO (Integration of Capabilities and Resources (N8)) or CMC (Deputy Commandants, Programs and Resources (DC,P&R) and Combat Development and Integration (DC,CD&I)).

From the date the ACAT I, IA, and II APBs are forwarded to CNO/CMC organizations, there is a 30-calendar day time limit to complete the concurrence/endorsement process. Concurrence will be assumed after 30 days unless a specific non-concurrence has been forwarded. For the ACAT I and II program APBs, OASN(RD&A)(AP&A) will coordinate the signatures and responses to ensure that the appropriate concurrences have been received.

IT program APBs will be endorsed by the IT functional area point of contact/manager.

1.2.1.2 <u>ACAT III and IV Endorsements</u>

ACAT III and IV program APBs will be prepared by the PM, endorsed by the PEO, SYSCOM Commander, or DRPM, as appropriate, the resource sponsor and IT functional area point of contact/manager and CMC (DC,CD&I) for Marine Corps programs; and approved by the MDA.

1.2.1.3 <u>Approval</u>

For ACAT I weapons systems programs, the APB will not be approved without the coordination of the Under Secretary of Defense (Comptroller) (**10 U.S.C. Section 2220(a)(2)**) and the Joint Requirements Oversight Council.

APBs will be prepared and approved at program initiation; revised and/or updated at each subsequent program decision point; and revised following an MDA-approved program restructure or an unrecoverable program deviation from the current APB. Any required changes to the APB resulting from one of these conditions will be processed and approved in the form of a revised APB. APBs are not to be updated for the sake of providing current information that is within the trade space between the established objective and threshold values.

The APBs for ACAT I and IA programs will be provided to OASN (RD&A) (Acquisition Programmatics and Analysis (AP&A)) in the CARS format.

1.2.2 OPNAV Processing Procedures

1.2.2.1 APB and CDD/CPD Coordination

For weapon systems programs, the PM will provide a copy of the draft APB to the RO/program sponsor for review and validation that the performance parameters are consistent with the approved CDD or CPD.

1.2.2.2 OPNAV Endorsement Procedures

The focal point for OPNAV review of APBs is the resource sponsor's requirements officer (RO), with whom the PM will coordinate during APB preparation. To facilitate the OPNAV review, the PM will supply copies of the APB to the RO for the review coordination. Close coordination between the RO and the CNO (N8) action officer is required for an expeditious OPNAV review. The RO will provide OPNAV comments to the PM and will attempt to resolve all OPNAV issues with the PM.

When staffing APBs for CNO (N8) endorsement, the resource sponsor should provide the additional following information to the CNO (N8) staff:

1. The reason for changing/updating the APB (i.e., to support a program/milestone decision point (providing the relationship of the decision to the overall progress of the program) or to document changes to program cost, schedule, and/or performance parameters that are outside the approved objective-threshold ranges);

2. The FYDP Budget display for the program with an indication regarding whether or not the program is fully funded across the FYDP in all appropriations (i.e., RDT&E, SCN, APN, etc.). Include a comparison of the program budget requirements versus budget authorized;

3. The last approved schedule of record for the program;

4. Any Congressional language or interest in the program or effort; and

5. Any technical, testing, or programmatic concerns that might impact the decision at hand.

1.3 APB Deviations Procedures

1.3.1 Program Deviations

A program deviation occurs when the PM has reason to believe that the current estimate of an APB cost, performance, or schedule parameter will breach the threshold value for that

parameter. When a program deviation occurs, the PM should immediately notify the MDA and the ACT for ACAT IC, IAC, and II programs or the equivalent team for ACAT III and IV programs.

Within 30 days of the program deviation, the PM should notify the MDA of the reason for the deviation and the action(s) being taken to bring the program back within the approved baseline thresholds. Within 90 days of the program deviation, the PM should:

1. Ensure the program is back within APB thresholds, or

2. Submit a new APB, changing only the breached parameter and those parameters directly affected by the breached parameter, or

3. Provide a date by which the new APB will be submitted or by which the program will be back within original APB thresholds.

4. Keep the CNO/CMC (DC,P&R and DC,CD&I) informed with regard to program deviations and baseline recovery actions.

1.3.2 Program Deviation Criteria

Unless otherwise specified, the value of a performance objective or threshold in the APB should not differ from the value for a like objective or threshold value in the CDD/CPD, and their definition should be consistent.

For weapon system programs the threshold value for schedule should normally be the objective value plus 6 months; and the threshold value for cost should normally be the objective value plus 10 percent.

1.3.3 Revised Baseline Approval

If a program cannot be brought back within the current APB, the PM prepares a revised APB, and obtains the same endorsements and approvals using the same procedures as required for the initial APB. For all ACAT programs, resource sponsors will review the APB deviation notification and commit to continued funding, if appropriate, by signing an OPNAV coordination sheet for the APB deviation notification.

1.4 Responsibilities

1.4.1 PM

The PM will maintain the currency and adequacy of the APB from program initiation until the program is no longer on the active ACAT program list. See SECNAVINST 5000.2D, paragraph 2.4 for discussion of active ACAT program list.

1.4.2 IT Functional Area POC/Manager

The IT functional area POC/manager/user's representative will:

1. Ensure KPPs from the CDD or CPD are extracted and included in the APB.

2. Ensure consistency with principal staff assistant's functional planning and target architecture.

3. Review and endorse the APB.

1.4.3 Resource Sponsor

1.4.3.1 ACAT I, IA, and II Programs

The CNO (N6 or N4 and N8) or CMC (DC,P&R and DC,CD&I) will endorse APBs and APB revisions.

1.4.3.2 ACAT III and IV programs

The resource sponsor and CMC (DC,CD&I) (for Marine Corps IT programs) will:

1. Endorse the APB.

2. Review and endorse all APB revisions.

1.4.4 MDA

The MDA will approve the initial APB and all APB revisions.

Acquisition Program Baseline Signature Page (Weapon System)

Classification

Acquisition Program Baseline
Program XXX

With the objective of enhancing program stability and controlling cost growth, we, the undersigned, approve this baseline document. Our intent is that the program be managed within the programmatic, schedule, and financial constraints identified. We agree to support, within the charter and authority of our respective official positions, the required funding in the Planning, Programming, Budgeting, and Execution System (PPBES).

This baseline document is a summary and does not provide detailed program requirements or content. It does, however, contain key performance, schedule, and cost parameters that are the basis for satisfying an identified capability need. As long as the program is being managed within the framework established by this baseline, in-phase reviews will not be held unless directed by the MDA.

_____
Program Manager (All ACAT programs) Date

_____
Program Executive Officer/SYSCOM/DRPM (All ACAT programs) Date
[If the MDA, signature should be after CNO/CMC]

_____
CNO (Program/Resource Sponsor) (All ACAT programs) Date
or CMC (Deputy Commandant, Combat Development and Integration) (All ACAT programs)

_____
CNO (Communication Networks (N6)) (ACAT I/II programs) Date
or CNO (Fleet Readiness and Logistics (N4)) (ACAT I/II programs)

_____
CNO (Integration of Capabilities and Resources (N8)) (ACAT I/II programs) Date
or CMC (Deputy Commandant, Programs and Resources) (ACAT I/II programs)

_____
ASN(RD&A) (ACAT I/II programs) Date

_____
Under Secretary of Defense (Acquisition, Technology Date
and Logistics) (ACAT ID programs)

Derived from:
Declassify on:

CLASSIFICATION

Acquisition Program Baseline Signature Page (IT System)

Classification

Acquisition Program Baseline
Program XXX

With the objective of enhancing program stability and controlling cost growth, we, the undersigned, approve this baseline document. Our intent is that the program be managed within the programmatic, schedule, and financial constraints identified. We agree to support, within the charter and authority of our respective official positions, the required funding in the Planning, Programming, Budgeting, and Execution System (PPBES).

This baseline document is a summary and does not provide detailed program requirements or content. It does, however, contain key performance, schedule, and cost parameters that are the basis for satisfying an identified capability need. As long as the program is being managed within the framework established by this baseline, in-phase reviews will not be held unless directed by the MDA.

Program Manager Date (All ACAT IT programs)	IT Functional Area POC/Manager Date (All ACAT IT programs)

Program Executive Officer/SYSCOM/DRPM (All ACAT IT programs) Date
[If the MDA, signature should be after CNO/CMC]

Program/Resource Sponsor (All ACAT IT programs) Date

CMC (Deputy Commandant, Combat Development and Integration) Date
(All USMC ACAT IT programs)

CNO (Integration of Capabilities and Resources (N8)) (ACAT IA programs) Date
or CMC (Deputy Commandant, Programs and Resources) (ACAT IA programs)

Milestone Decision Authority Date
(ACAT IAC and ACAT III and IVT IT programs)

ASN(RD&A), or designee Date
(ACAT IAM programs)

Assistant Secretary of Defense (Networks and Information Integration) Date
(ACAT IAM programs)
Derived from:
Declassify on:

CLASSIFICATION

Chapter 4
Information Technology (IT) Considerations

References:
(a) SECNAVINST 5000.2D
(b) DOD Instruction 5000.02, Operation of the Defense Acquisition System, of 8 Dec 08
(c) Department of Defense Architecture Framework (DoDAF) Ver 1.5 documents, 23 Apr 07 (NOTAL)
(d) Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3170.01C, Operation of the Joint Capabilities Integration and Development System, of 1 May 07
(e) DOD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), of 5 May 04
(f) DOD Directive 8500.01E, Information Assurance, of 24 Oct 02
(g) DOD Instruction 8500.2, Information Assurance (IA) Implementation, of 6 Feb 03
(h) DOD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), of 28 Nov 07
(i) SECNAVINST 5239.3A
(j) Chairman of the Joint Chiefs of Staff Instruction 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems, of 8 Mar 06
(k) DOD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management, of 15 Aug 04
(l) DOD Manual 8570.01-M, Information Assurance Workforce Management Program, of 19 Dec 05
(m) OPNAVINST 5100.23G

4.1 Clinger-Cohen Act (CCA) (40 U.S.C., Subtitle III) Compliance

4.1.1 CCA Compliance Package Development and Processing for ACAT IAM, IAC, ID, IC, and II Programs containing Mission-Critical (MC) or Mission-Essential (ME) IT Systems including National Security Systems (NSS)

CCA compliance certification or confirmation, as appropriate, shall be obtained through the process described in reference (a), enclosure (4), paragraph 4.1.

4.1.2 CCA Compliance Package Development and Processing for ACAT III, IV, and Abbreviated Acquisition Program (AAP) Programs containing MC or ME IT Systems including NSS

CCA compliance confirmation shall be obtained through the process described in reference (a), enclosure (4), paragraph 4.1.

4.2 <u>Contracts for Acquisition of MC or ME IT Systems including NSS</u>

[*fm SNI 5000.2D, 4.2: No contract shall be awarded that acquires an MC or ME IT system, including an NSS, until:*

1. The IT system is registered in the DON IT Registration Database (Contact your Command IO for assistance with IT Registration),

2. The Information Assurance Strategy is coordinated with the DoD CIO for ACAT ID, IAM, and IAC programs, and approved by the DON CIO for ACAT ID, IC, IAM, IAC, and II programs, or by the respective Command IO for ACAT III, IV, and abbreviated acquisition program (AAP) programs, (A PEO program manager or DRPM may have their ACAT III, IV, and AAP program Information Assurance Strategy approved by the DON CIO.), and

3. Compliance with the CCA is certified for ACAT IAM and IAC programs and confirmed for ACAT ID, IC, II, III, IV, and AAP programs.

4. When the use of commercial IT is considered viable, maximum leverage of and coordination with the DoD Enterprise Software Initiative (DoD ESI) and the Federal SmartBUY shall be made. The DoD ESI is an initiative led by the DoD CIO to develop processes for DoD-wide software asset management. The DoD implements SmartBUY through the DoD ESI Team, which provides DoD commercial software requirements to SmartBUY and manages selected SmartBUY agreements. DoD ESI and SmartBUY have jointly established software agreements for commercial software and software maintenance that coordinate multiple IT investments to leverage the Federal Government's purchasing power for best-priced, standards-compliant products. Neither DoD ESI nor SmartBUY mandate use of particular brands of software, but DON activities purchasing software for which agreements have been awarded must follow DFARS 208.74 and consider use of DoD ESI agreements before buying elsewhere, and if there are existing SmartBUY agreements, they must use the SmartBUY agreements. The Web site http://www.esi.mil/ provides additional guidance.]

See reference (b), enclosure 5, for implementation requirements for all Department of the Navy (DON) acquisition category (ACAT) programs.

4.3 <u>Information Integration and Interoperability</u>

Consideration shall be given to information interoperability products described in reference (c), the Department of Defense Architecture Framework Document, in the creation of capability development/production documents (CDD/CPDs). Interoperability at the data level is essential for

information superiority; the DON data management and interoperability (DMI) engineering and management processes are essential in improving interoperability at this level.

Within an information technology (IT), including NSS, program, program managers (PMs) should characterize information interoperability by extracting the information exchange requirements from the CDD/CPD along with the associated interoperability/Net-Ready Key Performance Parameters (KPPs). This characterization, using mission-area integrated architectures as described in references (d) and (e), will also be in the context of either a family of systems (FoS) or a systems of systems (SoS), and a mission area, and shall apply to all IT systems, including NSS.

4.4 Information Assurance (IA) Program Manager (PM) Responsibilities

Information Assurance (IA) is the cornerstone to the DON transformation to a secure interoperable, net-centric Naval Information Management (IM)/ IT Enterprise. The security and superiority of DON information, systems, and personnel are key to maritime dominance and national security. The DON takes a Defense in Depth (DID) approach to IA, layering IA principles and controls that apply to people, processes, and technology.

IA is the defensive component of information operations (IO). IA protects and defends information and information systems (IS) by ensuring their availability, integrity, confidentiality, authentication and non-repudiation. IA includes providing for the restoration of IS by incorporating protection, detection and reaction capabilities. The more interoperable and information dependent DON Operations become, the more important IA becomes. Without effective IA, "full spectrum dominance" in the information domain is not achievable. Simply disrupting the network isolates sensors from weapon systems and impairs naval warfighting ability. Infiltrating the network allows the enemy to exploit sensors and understand force disposition.

PMs should manage and engineer information systems using the best processes and practices known to reduce security risks, including the risks to timely accreditation. Per references (f), (g), (h), and (i), PMs shall address IA requirements throughout the life-cycle of all DoD IT systems, including NSS. The PM shall incorporate IA control measures (safeguards) into IT systems, including NSS, based upon approved CDD/CPD-derived mission assurance category (MAC) and confidentiality level (CL). Minimum control measures described in reference (g) ensure that appropriate levels of availability, integrity, authentication, confidentiality, and non-repudiation are sustained. These controls will also allow the system protection against information attack, and when it occurs, detect, respond, and restore the system to full functionality. The security certification and accreditation (C&A) process will ensure that,

based upon MAC and CL, the appropriate security safeguards are properly implemented. References (f) and (g) establish the minimum IA capabilities that are to be incorporated in DoD information systems and connected IT systems, including NSS. PMs should ensure that the MAC and CL are identified in the acquisition strategy.

SECNAV Manual 5239.1, Department of the Navy Information Assurance Program: Information Assurance Manual, Nov 05, describes the roles and responsibilities of PMs, Information Assurance Managers (IAM), and other key individuals who provide IA services and are important to a successful DON IA program.

4.4.1 Information Assurance and Integrated Architectures

Systems must exchange information within the confines of the integrated Navy architectures and the global information grid (GIG). Program managers should use the ASD(NII) Net-Centric Checklist version 2.1.3. of 12 May 04 to understand the net-centric attributes that their IT, including NSS, programs need to implement to move into the net-centric environment as part of integrated Navy architecture in the GIG. A service-oriented, integrated Navy architecture is a design style for building flexible, adaptable distributed-computing environments for the Department of Defense (DoD). Service-oriented, integrated Navy architecture design is fundamentally about sharing and reuse of functionality across diverse applications. IT systems, including NSS, must be procured with appropriate IA controls so that they are "Net-Ready" to be inserted into integrated Navy architectures. IA control measures must be designed into systems with careful consideration of the context in which the integrated architectures will function. Information assurance hardware and software capabilities (tools) must be assessed for and meet interoperability requirements as established by the Information Assurance Panel as stated in reference (j). Service and joint interoperability requirements establish the context within which information is exchanged and impact IA controls. Electromagnetic environmental effects (E3) impact information availability and integrity. Radio frequency (RF) spectrum must be reserved, available, and managed. The system security certification and accreditation (C&A) process must verify and validate IA controls in the context of architecture within which it will function. Net-readiness, E3, spectrum management, system security C&A and IA are interdependent and must be incorporated into IT systems, including NSS, from an integrated architectural perspective.

4.4.2 IA Strategy Content

4.4.2.1 Policies, Standards, and Architectures

Describe how IT, including NSS, program information assurance features are consistent with DoD policies, standards, and architectures.

4.4.2.1.1 Benchmark

1. Minimum DoD IA requirements are defined in references (f) and (g).

2. MAC and CL specify the confidentiality, availability, and integrity minimum requirements for a DoD information system and a connected IT system, including NSS.

3. IA capabilities requirements should be specified in the capability development/production document (CDD/CPD) as MAC and CL and incorporated into IT, including NSS, program design activities.

4. Interoperability requirements affected by the IA design approach are specified (see reference (g)).

5. Program requirements for support from the DoD IA infrastructure (e.g., public key infrastructure) are specified.

6. The impact of DoD Cryptographic Modernization Program upon cryptographic functions is addressed.

7. System certification testing is conducted to ensure that CDD/CPD stated MAC and CL security requirements are met.

8. Information system survivability is addressed by incorporating protection, detection, reaction, and reconstitution capabilities into the system design.

9. Relevant DON/DoD policies concerning the use of evaluated Commercial-Off-The-Shelf (COTS)/government-off-the-shelf (GOTS) IA products per reference (g) are identified.

10. Information assurance requirements are addressed throughout an IT, including NSS, program’s life-cycle.

11. To the extent possible, the requirements of the Navy/Marine Corps Unclassified Trusted Network Protection Policy (UTNProtect Policy) need to be supported. Specifically, the ports, protocols, services, and conditions for use referenced in the Navy/Marine Corps UTNProtect Policy (https://infosec.navy.mil) need to be considered. Recommended COTS product evaluations that could support the Navy/Marine Corps UTNProtect Policy can also be found at https://infosec.navy.mil/.

4.4.2.1.2 Potential Sources

IT, including NSS, command, control, communications, computers, and intelligence support plan (C4ISP)/information support plan (ISP), Net-Ready Key Performance Parameter (NR-KPP) per reference (e), system security authorization agreement (SSAA), and CDD/CPD are potential sources.

4.4.2.2 Certification and Accreditation

Describe the overall certification and accreditation approach.

4.4.2.2.1 Benchmark

1. All security requirements are included in the testing strategy for developmental test and evaluation (DT&E) and operational test and evaluation (OT&E),

2. Successful certification and accreditation of the information system per the DIACAP as defined in reference (h).

3. The responsible Designated Approving Authorities (DAAs) are identified,

4. There is agreement with the DAA(s) on the certification and accreditation approach (e.g., a system, type, or site certification process to be used), and

5. The status of the program SSAA per the DITSCAP is identified.

4.4.2.2.2 Potential Sources

IT, including NSS, C4ISP/ISP, SSAA, and test and evaluation master plan (TEMP).

4.4.3 IA Workforce

Identifying and categorizing positions conducting IA activities in support of the GIG, and certifications required of those positions, is governed by references (k) and (l). Program Managers should review these issuances to ensure their program adheres to all procedures and requirements applicable to the IA workforce, including contracted support. The PM should be aware that since references (k) and (l) impact contracted support, SECNAVINST 5000.2D, enclosure (8), should also be consulted.

4.5 Records Management

4.6 Human Systems Integration and Environment, Safety, and Occupational Health (ESOH) Considerations

PMs of IT systems should evaluate the ESOH requirements and considerations during design, development, and installation/deployment of computer software and hardware, including the incorporation of human systems integration and ergonomics considerations per references (a) and (m). Software safety risks for critical control and display systems should be evaluated using MIL-STD-882D. As with other systems acquisition, demilitarization and disposal planning for IT systems should include ESOH considerations and potential environmental impacts.

Chapter 5
Integrated Test and Evaluation

References:
(a) DOD 5000.3-M-4, Joint Test and Evaluation Procedures Manual, of 1 Aug 88
(b) DOD Instruction 5000.02, Operation of the Defense Acquisition System, of 8 Dec 08
(c) SECNAVINST 5200.40
(d) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems, of 8 Mar 06
(e) DOD Instruction 8500.2, Information Assurance Implementation, of 6 Feb 03
(f) DOD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), of 28 Nov 07
(g) SECNAVINST 5239.3A
(h) OPNAVINST 2400.20F
(i) 32 CFR 775, Procedures For Implementing The National Environmental Policy Act
(j) 32 CFR 187, Environmental Effects Abroad of Major Department of Defense Actions
(k) Assistant Secretary of the Navy (Installations and Environment) Memorandum 99-01, Requirements for Environmental Considerations in Test Site Selection, of 11 May 99
(l) OPNAVINST 5090.1C
(m) DOD Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), of 30 Jun 04
(n) SECNAVINST 5000.36A
(o) SECNAVINST 5100.10J
(p) OPNAVINST 5100.8G
(q) OPNAVINST 5100.19E
(r) OPNAVINST 5100.23G
(s) OPNAVINST 5100.24B
(t) DOD Directive 5230.20, Visits and Assignments of Foreign Nationals, of 22 Jun 05
(u) OPNAVINST 9072.2
(v) SECNAV M-5510.36
(w) DOD Directive 3200.12, DoD Scientific and Technical Information (STI) Program (STIP), of 11 Feb 98

Chapter 5 Preamble

This chapter has been organized with the intent to localize as much test and evaluation information as possible for the reader. All information in Chapter 5 of SECNAVINST 5000.2D has been incorporated into this chapter of the guidebook. The

information from SECNAVINST 5000.2D is annotated within brackets and **bold**, **italicized** print. SECNAVINST 5000.2D content begins with a bracket, the italicized acronym *fm SNI 5000.2D*, with the appropriate SECNAVINST paragraph number followed by a colon, the content, and ends with a bracket (i.e. [***fm SNI 5000.2D, 5.1: text content from instruction***]). References letters (a, b, etc.) from SECNAVINST 5000.2D within the brackets have been modified as necessary to track to the correct reference at the beginning of this guidebook enclosure/chapter. Additional guidance and supporting information is in Courier 12 print outside the brackets.

5.1 Integrated Test and Evaluation (T&E) Overview

[***fm SNI 5000.2D, 5.1: T&E is conducted continuously throughout the acquisition life cycle of a system:***

1. For statutory and regulatory reasons, and

2. To gain knowledge that can be used to:

a. Advance system development,

b. Make programmatic acquisition decisions, and

c. Inform users about the system's operational characteristics and performance.

This enclosure delineates the mandatory T&E roles, responsibilities, procedures, and requirements for Department of Navy acquisition programs. While T&E is divided into contractor, developmental, operational, and live fire testing, it shall be integrated and coordinated with the users, the system developers, and the testers to the fullest extent allowed by statute and regulation. The integration and coordination of T&E shall start early, preferably during concept refinement. Where mandatory T&E procedures and requirements are not provided for herein or need clarification, guidance shall be requested for Navy programs from the Chief of Naval Operations (CNO), Director of Test & Evaluation and Technology Requirements (N091), or for Marine Corps programs from the Director, Marine Corps Test and Evaluation Activity (MCOTEA).]

Definition: "Integrated Testing" is the collaborative planning and collaborative execution of test phases and events to provide data in support of independent analysis, evaluation, and reporting by all stakeholders particularly the developmental (both contractor and government) and operational test communities.

Execution: All programs should establish a team made up of all relevant organizations (including contractors, developmental and operational test communities) to create and

manage an integrated T&E Strategy that will be incorporated into the Test and Evaluation Master Plan (TEMP). The team is established as early as possible in the program, preferably during the concept refinement phase, to collaboratively identify test parameters, data, and resources required for the development of the DT and OT plans and other required certifications (i.e., interoperability, system assurance, anti-tamper, safety, etc) to optimize test data collection while minimizing test resource requirements. The intent is to increase the overall efficiency of testing, improve product performance, and decrease the acquisition timeline. The Milestone Decision Authority (MDA) will provide formal direction establishing the test team in the program's Acquisition Decision Memorandum. As appropriate, contractor participation in the integrated test planning and execution will be included in Requests for Proposals (RFPs) and subsequent contracts.

The test requirements of this enclosure should be tailored for shipbuilding programs beyond legacy Milestone II/low-rate initial production (LRIP).

5.2 DON Points of Contact and Responsibilities for T&E

[***fm SNI 5000.2D, 5.2: To effect an efficient forum for collaboration, personnel who participate in test and evaluation processes for the DON must have fundamental knowledge of the DoD practice of Integrated Product Teams (IPTs) and the responsibilities of organizations contained in this instruction. The responsibilities contained herein are not meant to be restrictive in nature, but to provide a common base for all T&E participants to communicate organization, plans, and execution. In addition to understanding the intent of T&E guidance provided in this instruction, DON personnel should utilize web-enabled knowledge forums to amplify their knowledge of standard and best practices, lessoned learned, and to ensure compliance with legal statutes and regulations.***]

5.2.1 Principal Navy Points of Contact and Responsibilities

5.2.1.1 Chief of Naval Operations (CNO) (N091) Director Test and Evaluation and Technology Requirements

[***fm SNI 5000.2D, 5.2.1.1: CNO (N091) is responsible to the CNO for establishing Navy T&E policy, determining the adequacy of T&E infrastructure required to support systems testing, coordinating Navy participation in joint testing matters, reviewing capabilities documents (e.g., Initial Capabilities Document (ICD), Capability Development Document/Capability Production Document (CDD/CPD)) for testability, and resolving developmental and operational test issues. CNO (N091) shall act as the final authority and signatory for Test and Evaluation Master Plans (TEMPs) prior to Component Acquisition Executive (CAE) approval and signature. CNO (N091) shall be responsible***

for overseeing testing matters associated with Marine Corps aircraft, aviation equipment, and Air Traffic Control And Landing (ATCAL) equipment.]

CNO (N912) Action Officers participate in T&E Working-level Integrated Product Teams (T&E WIPT) (see paragraph 5.4.3); and when necessary, convene a Test and Evaluation Coordination Group (TECG) as discussed in paragraph 5.4.4.

CNO (N091) is also responsible for:

1. Coordinating operational test and evaluation (OT&E) support for the United States Marine Corps (USMC),

2. Providing principal liaison with Commander, Operational Test and Evaluation Force (COMOPTEVFOR) on operational test requirements and execution.

3. Acting for CNO as the single point of contact for interface with DoD's Director, Operational Test and Evaluation (DOT&E) for all T&E policy issues and all matters related to the test and evaluation master plan (TEMP) and test plan coordination and approval,

4. Acting for CNO as the single point of contact for interface with DoD’s Developmental Test and Evaluation (DT&E) office for all T&E policy issues and all matters regarding TEMP coordination and approval,

5. Serving as the Office of the Chief of Naval Operations (OPNAV) point of contact with the Office of the Secretary of Defense (OSD) on joint service testing matters conducted per reference (a),

6. Serving as the Navy LFT&E primary point of contact, and

7. Serving as the principal interface between CNO and Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN(RD&A)), on matters relating to T&E.

5.2.1.2 <u>Program Manager (PM)</u>

[***fm SNI 5000.2D, 5.2.1.2: The PM shall, in concert with the developer, user, and testing communities, coordinate developmental test and evaluation (DT&E), Operational Test and Evaluation (OT&E), and Live-Fire Test and Evaluation (LFT&E) into an efficient continuum, closely integrated with system design, development, production, and sustainment, that achieves the approved capability. The necessary time and resources shall be***

planned and budgeted to ensure adequate testing is conducted to support decision makers and the Fleet throughout the life cycle of the acquisition.]

The PM should advise the decision authority that the program is ready for operational testing and initiate an operational test readiness review (OTRR) to certify the program ready for the next phase of independent operational testing.

5.2.1.2.1 <u>Personnel Security Clearances</u>

When programs involve security measures that require special consideration (i.e. new technologies, anti-tamper, Special Compartmented Information or Access Programs), the PM should ensure adequate lead-time is provided for testing agencies, in particular operational test agents, to identify subject matter experts who qualify and are granted access to information that will allow independent preparation for T&E strategies and plans. When billets are limited or restricted, the PM is responsible for coordinating an adequate billet structure to support testing.

5.2.1.3 <u>Commander, Operational Test and Evaluation Force (COMOPTEVFOR)</u>

[***fm SNI 5000.2D, 5.2.1.3: COMOPTEVFOR is the designated Operational Test Agency (OTA) for the United States Navy and for Marine Corps aviation programs assigned to CNO sponsorship. COMOPTEVFOR shall: plan, conduct, evaluate, and report the OT&E of Acquisition Category (ACAT) I, IA, II, III, IVT, and Rapid Deployment Capability (RDC) programs; monitor ACAT IVM programs; evaluate initial tactics for systems that undergo OT&E; and make fleet release or introduction recommendations to CNO for all ACAT programs and those system configuration changes selected for OT&E. COMOPTEVFOR prepares the OT&E content (normally Part IV) and a section listing operational test resources needed to execute test (normally incorporated in Part V) with the exception of live fire test and evaluation (LFT&E) for the Test and Evaluation Master Plan (TEMP). COMOPTEVFOR shall coordinate for multi-service and joint OT&E, and is the lead OTA when the Navy is assigned lead. COMOPTEVFOR is the designated RDT&E fleet-support scheduling agent for CNO (N091).***]

In addition, COMOPTEVFOR:

1. Serves as an advisor to CNO on DON matters pertaining to OT&E,

2. Coordinates the scheduling of resources for OT,

3. Identifies significant test limitations and advises the CNO (N091), other CNO codes as desired, and MDA of risk associated in the procurement decision,

4. Coordinates Navy support of other military Services' OT&E,

5. Assists in the conduct of DT&E monitoring and commenting on relevant OT&E issues, and

6. Ensures that operations and system security requirements are met for all OT&E evolutions.

5.2.1.4 Naval Systems Commands (SYSCOMs)

[***fm SNI 5000.2D, 5.2.1.4: SYSCOMs shall manage assigned facilities and personnel to ensure efficient and effective integration of DT&E and LFT&E of systems within the SYSCOM's domain. When requested and funded, SYSCOMs will support programs with the resources needed to coordinate planning, scheduling, and executing T&E throughout the continuum of system development.***]

5.2.1.4.1 Naval Air Systems Command (NAVAIRSYSCOM)

[***fm SNI 5000.2D, 5.2.1.4.1: NAVAIRSYSCOM, in support of PMs, shall conduct and report on DT&E and LFT&E of Navy and CNO sponsored Marine Corps aircraft, aviation systems, and ATCAL equipment.***]

5.2.1.4.1.1 Naval Air Systems Command Technical Assurance Board (NTAB)

[***fm SNI 5000.2D, 5.2.1.4.1.1: The NTAB shall monitor emerging aircraft and aircraft-related programs under development. All aircraft ACAT I Naval Aviation programs and other select programs when requested by the Developing Activity (DA), the resource sponsor, or CNO (N091) shall be monitored until completion of Initial Operational Test and Evaluation (IOT&E). Monitoring shall continue until all major deficiencies are resolved or the program is removed from the Major Defense Acquisition Program (MDAP) list.***]

NAVAIR INSTRUCTION 3960.5 provides policies, procedures, and responsibilities for the NTAB monitoring of aircraft weapon system development. In addition, NTAB should:

1. Report and classify deficiencies as NTAB deficiencies according to COMNAVAIRSYSCOM instructions (Yellow sheet reporting instructions).

2. In the event that NTAB Part I deficiencies are temporarily waived or deferred per SECNAVINST 5000.2D, enclosure

(5), paragraph 5.6.4, continue monitoring until commencement of first deployment.

3. Provide subject matter expertise in T&E WIPT process.

5.2.1.4.2 Weapons System Explosive Safety Review Board (WSESRB)

[***fm SNI 5000.2D, 5.2.14.2: The WSESRB is the Navy's independent agent for assessing energetic systems, weapons, and those systems that manage and control weapons for safety compliance. WSESRB review findings provide the fundamental explosives safety input for the conduct of final developmental and operational testing and for major acquisition decisions.***]

NAVSEA INSTRUCTION 8020.6E provides membership, responsibilities and procedures for the WSESRB. DON programs that develop or utilize energetic elements or systems that interface with energetic systems should consult with the WSESRB in the Concept Refinement phase or earlier.

5.2.1.4.3 Space and Naval Warfare Systems Command (SPAWAR) Office of the Chief Engineer (CHENG)

The SPAWAR CHENG serves as the principal subject matter expert for T&E of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems throughout the SPAWAR domain. This office supports the T&E WIPT process to ensure statutory, regulatory, and all other testing objectives, including joint interoperability and other certifications are accomplished. The SPAWAR CHENG also advises decision authorities as to the resolution/status of these objectives before major program decisions.

5.2.1.5 Office of Naval Intelligence (ONI)

[***fm SNI 5000.2D, 5.2.1.5: ONI is the designated naval activity responsible for threat intelligence and validating threat tactics supporting T&E of Navy acquisition programs. For ACAT ID programs, ONI threat assessments will be validated by the Defense Intelligence Agency (DIA) per reference (b).***]

5.2.2 Principal Marine Corps Points of Contact and Responsibilities

5.2.2.1 Deputy Commandant for Manpower and Reserve Affairs (DC,M&RA)

[***fm SNI 5000.2D, 5.2.2.2: DC,M&RA assigns personnel per established manpower requirements for Marine Corps participation in JT&E and in support of OT&E for ACAT I and designated ACAT II programs within manpower guidelines established by the Deputy Commandant, Combat Development and Integration (DC,CD&I) and***

after consultation with Commanding General, Marine Corps Systems Command (CG, MARCORSYSCOM) and the Director, Marine Corps Operational Test and Evaluation Activity (MCOTEA).

DC,M&RA is designated the functional manager for Marine Corps Manpower Systems' Automated Information Systems (AISs). DC,M&RA is responsible for developing the concept of employment (COE) and Mission Essential (ME) functions for Manpower AISs and interoperability and standards requirements for Capability Development/Production Documents (CDDs/CPDs). DC,M&RA will provide representatives to coordinate with CG, MARCORSYSCOM, the Marine Corps Direct Reporting Program Managers (DRPMs), and Director, MCOTEA, to assist in determining AIS program failure definition (FD)/scoring criteria (SC) for each manpower system's AIS program under development and provide a voting member for scoring conferences.]

DC,M&RA assigns:

1. USMC participants in joint test and evaluation (JT&E),

2. A Test Director (TD) for OT&E of ACAT I and designated ACAT II programs,

3. A Deputy TD for multi-service OT&E of ACAT I programs, and

4. A Deputy TD for JT&E-approved programs as appropriate.

When the required structure for items (2), (3), and (4) above is not on the Joint Duty Assignment List (JDAL), a compensated structure validation should be completed through MCCDC (Total Force Structure Division (TFSD)) and the Joint Staff.

5.2.2.2 <u>Deputy Commandant for Installations and Logistics (DC,I&L)</u>

[***fm SNI 5000.2D, 5.2.2.2: DC,(I&L) is designated the functional manager for Marine Corps Logistics Systems' AISs.***] DC,I&L is responsible for:

1. Developing the COE and mission essential functions for Logistics AISs and interoperability and standards requirements for capability development/production documents (CDD/CPDs);

2. Providing a representative to coordinate with CG, MARCORSYSCOM, the Marine Corps DRPMs, and Director, MCOTEA, in

determining AIS program failure definition (FD)/scoring criteria (SC) for each Logistics System's AIS program under development; and

3. Providing a voting member for scoring conferences.

5.2.2.3 <u>Director, Marine Corps Intelligence Activity (MCIA)</u>

[***fm SNI 5000.2D, 5.2.2.3: Director, MCIA shall provide CG, MARCORSYSCOM, Marine Corps DRPMs, and Director, MCOTEA with a threat test support package (TTSP) based on the latest system threat assessment (STA). The TTSP should include all threat data required to support DT, OT and LFT&E.***]

5.2.2.4 <u>Deputy Commandant, Combat Development and Integration (DC,CD&I)</u>

[***fm SNI 5000.2D, 5.2.2.4: DC,CD&I shall develop the concept of employment (COE), Operational Mode Summary/Mission Profiles (OMS/MP), and ME functions for proposed non-automated information systems and interoperability and standards requirements for CDDs/CPDs. In coordination with CG, MARCORSYSCOM, the Marine Corps DRPMs, and Director, MCOTEA, provide a representative to assist in determining non-AIS program FD/SC for each program under development and provide a voting member for scoring conferences.***

DC,CD&I provides oversight of joint test and evaluation (JT&E) for the Commandant of the Marine Corps (CMC) and Headquarters Marine Corps (HQMC) Staff to ensure T&E activities directly support the CMC's responsibilities for sustained material readiness and mission capability of the Fleet Marine Force (FMF). DC,CD&I will be the primary interface with Joint Interoperability Test Command (JITC) for all joint test and evaluation issues.]

5.2.2.5 <u>Commanding General, Marine Corps Systems Command (CG, MARCORSYSCOM)</u>

[***fm SNI 5000.2D, 5.2.2.5: CG, MARCORSYSCOM shall budget for DT&E and OT&E and act as the focal point for interface with the Board of Operating Directors for Test and Evaluation (BoOD(T&E)). CG, MARCORSYSCOM provides oversight of programming activities related to T&E for the CMC and HQMC Staff to ensure T&E activities directly support the CMC's responsibilities for sustained material readiness and mission capability of the Fleet Marine Force (FMF). The CG, MARCORSYSCOM PM shall provide a test support package (TSP) to the Director, MCOTEA, one year before scheduled OT start. The TSP should include, at a minimum, early T&E, a CDD/CPD, a STA, a threat scenario, a DC,CD&I-approved COE, program documentation addressing support, and life-cycle management of hardware and computer resources and an***

organizational structure to include a table of organization and table of equipment. Upon request, the PM should provide software documentation. The threat scenario must include a signed concurrence from MCIA. CG, MARCORSYSCOM serves as the Marine Corps point of contact with Office of the Secretary of Defense (OSD) on matters relating to LFT&E. CG, MARCORSYSCOM shall consolidate and process quarterly requests for use of naval fleet assets in support of Research, Development, Test, and Evaluation (RDT&E) requirements. CG, MARCORSYSCOM shall represent the Marine Corps in all DT&E matters. CG, MARCORSYSCOM shall be the primary interface with JITC on joint interoperability testing conducted during DT. CG, MARCORSYSCOM shall exercise review and approval authority over TEMPs for assigned programs and multi-service programs. CG, MARCORSYSCOM shall establish and chair a Test and Evaluation Working Integrated Product Team (T&E WIPT)for all assigned programs. CG, MARCORSYSCOM shall certify that systems are safe and ready for DT&E and OT&E. CG, MARCORSYSCOM shall manage the Marine Corps External Airlift Transportation (EAT) Certification Program and the Marine Corps Foreign Comparative Testing Program.]

5.2.2.6 <u>Director, Marine Corps Operational Test and Evaluation Activity (MCOTEA)</u>

[*fm SNI 5000.2D, 5.2.2.6: MCOTEA is the designated OTA for the United States Marine Corps. Director, MCOTEA shall ensure that the OT of all ACAT programs is effectively planned, conducted, evaluated, and reported; and shall coordinate the scheduling of resources for OT requiring FMF support through the Two Year Master Test Plan (TYMTP) published annually with quarterly updates. Director, MCOTEA shall host and chair a T&E WIPT for determining FD/SC for each program. Director, MCOTEA shall prepare Part IV of the TEMP with the exception of LFT&E. Director, MCOTEA shall request, from CMC, the assignment of a Test Director (TD) for ACAT I and certain ACAT II programs. Director, MCOTEA shall task the FMF and other commands in matters related to OT&E by publishing a Test Planning Document (TPD). When significant test limitations are identified, the Director, MCOTEA, shall advise the MDA of risk associated in the procurement decision. Director, MCOTEA shall manage those OSD-directed Multi-Service OT&Es for which the Marine Corps is tasked. Director, MCOTEA shall chair and conduct an operational test readiness review (OTRR) for determining a program's readiness to proceed with OT&E. See this instruction (SECNAVINST 5000.2D), enclosure (5), paragraph 5.6, for further guidance. Director, MCOTEA shall prepare and provide directly to the CMC, within 90 days after completion of OT&E, an independent evaluation report for all OT&E. Director, MCOTEA shall coordinate Marine Corps support for other military services' OT&Es. Director, MCOTEA shall advise the Assistant Commandant of the Marine Corps (ACMC) on OT&E matters. Director, MCOTEA shall chair an annual OT&E planning conference. The conference should have representation from the Marine Forces, appropriate HQMC*

staff offices, DC,CD&I, CG, MARCORSYSCOM, and others, as appropriate. Director, MCOTEA shall maintain direct liaison with OSD's Director, Direct of Operational Test and Evaluation (DOT&E), the FMF for OT&E matters, and other military activities and commands, as required. Director, MCOTEA shall represent the Marine Corps in all Multi-Service OT&E matters. Director, MCOTEA shall be the primary interface with JITC on joint interoperability testing conducted during OT. For USMC programs not required by statute to conduct LFT&E, but where LFT&E is appropriate, the Director, MCOTEA shall concur with the LFT&E strategy as approved by the MDA in the Test and Evaluation Strategy (TES) or TEMP.]

5.2.2.7 Marine Forces

[***fm SNI 5000.2D, 5.2.2.7: The Commanding Generals, Marine Forces Pacific (MARFORPAC) and Marine Forces Command (MARFORCOM) shall designate a test coordinator as a focal point for all T&E matters and support MCOTEA in the T&E of new concepts, equipment, and systems. The Marine Forces shall provide a TD who will write the OT report and submit it to MCOTEA via the CG of the appropriate Marine Forces within 30 days of completion of OT&E for an ACAT II, III, or IV program. The Marine Forces shall provide personnel and equipment to participate in JT&E programs, as required.***]

5.2.3 Acquisition Items Exempt from T&E Provisions within this Instruction (SECNAVINST 5000.2D)

5.2.3.1 Items Exempt

[***fm SNI 5000.2D, 5.2.3.1: The following items are tested by other organizations and are exempt from the T&E provisions of this instruction (SNI 5000.2D):***

1. Cryptographic or Cryptology equipment

2. Naval Nuclear Reactors and associated Systems

3. Nuclear Weapons

4. Medical and Dental Systems

5. Spacecraft and Space-based systems.]

5.2.3.2 T&E Considerations that Apply to Exempt Items

[***fm SNI 5000.2D, 5.2.3.2: The exemption herein does not apply to the following aspects of these items:***

1. Information Technology (IT) administrative systems

2. Ships or Aircraft that carry these systems

3. Other systems that these exempt items support

4. Testing conducted at the request of or in cooperation with above parent organizations

When the performance of these exempted items affects the effectiveness, suitability, survivability, or lethality of a system not exempt (e.g., communications system with embedded cryptology subsystem, ship with nuclear propulsion), then the exempted item's performance may be considered in the T&E of the supported system. Such performance assessments must be coordinated with and approved by the organization with direct responsibility for the exempted item (e.g., National Security Agency (NSA) for cryptology systems or naval reactors for naval nuclear propulsion systems).]

5.3 T&E Strategy

5.3.1 Preparation and Milestones

[***fm SNI 5000.2D, 5.3.1: See reference (b), enclosure 5, for guidance in preparing a T&E strategy (TES) that is required at Milestone A. The TES documents a strategy of realistic test concepts that support development decisions throughout the acquisition life-cycle. The TES must include adequate detail to construct pre-Milestone B assessments and tests. The TES is the precursor to the TEMP that is required for Milestone B and beyond. While specific program alternatives are generally unknown before Milestone B, the TES needs to address: the maturity level of the technology; anticipated DT&E, OT&E, and LFT&E concepts; and early predictions of test support requirements that may need development or procurement. When Modeling and Simulation (M&S) is part of the T&E strategy, the M&S proponent shall provide the strategy to comply with verification, validation and accreditation per reference (c). For OT&E events prior to Milestone B, the T&E strategy shall identify objectives, scope, and funding, as well as overall evaluation strategy. Programs shall conform to DOT&E policies and guidelines when preparing TES documentation, unless granted relief by the TEMP approval authority.***]

5.3.2 Strategy Approval

[***fm SNI 5000.2D, 5.3.2: The T&E strategies for programs on the OSD T&E Oversight List require the approval of DOT&E and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L). Programs on the OSD T&E Oversight List will prepare a T&E strategy and coordinate with CNO (N091) or Director, MCOTEA for submission via the same approval process for a TEMP.***]

See paragraph 5.4.7.14 of this guidebook for routing the

TEMP for approval and Annex 5-A for the signature cover pages associated with the appropriate ACAT level program.

5.4 T&E Planning

5.4.1 Early Planning for Integrated T&E

[*fm SNI 5000.2D, 5.4.1: Early involvement by test agencies is required to ensure successful execution of integrated testing. The DA, test agencies, and user representative (resource sponsor) must share a common interpretation of the system capability needs so that DT and OT are tailored to optimize resources, test scope, and schedule. Early, active, and continuous participation by test agencies during the development of capabilities documents will support effective communication and common interpretation.*]

5.4.2 Testing Increments in Evolutionary Acquisition

[*fm SNI 5000.2D, 5.4.2: Developing Agencies shall ensure adequate DT&E, OT&E, and LFT&E are planned, funded, and executed for each new increment capability, as required. The PM shall ensure an independent phase of OT&E prior to release of each increment to the user. Potentially short cycle times between milestone decisions necessitate early collaboration between the OTA, JITC, test resource providers (labs, ranges, instrumentation sources, etc.), sponsors, requirements officers, and oversight agencies in test planning for efficiency and testability that effectively evaluates system capabilities and performance. In addition to integrating test events to the fullest extent within statute and regulation, planners shall consider parallel development and review of the TEMP and the relevant capabilities documents (e.g., CDD/CPD).*]

5.4.2.1 Innovative Testing

[*fm SNI 5000.2D, 5.4.2.1: Short incremental development or spiral development cycle times and simultaneous testing of multiple increments may require innovative methods not discussed in this or other acquisition documents. Innovative or irregular methods will be described within the appropriate sections of the TEMP. TEMP concurrence and approval will formalize the agreement to implement those methods for use in the program.*]

5.4.2.2 Initial Operational Test and Evaluation (IOT&E)

[*fm SNI 5000.2D, 5.4.2.2: The PM shall ensure IOT&E is completed prior to proceeding beyond Low Rate Initial Production (LRIP) as required by Title 10 U.S.C., Section 2399 and for all other programs on the OSD T&E oversight list as required by reference (b). The PM shall ensure OT&E is conducted for each evolutionary acquisition increment for programs requiring OT&E. DOT&E, for programs on the OSD T&E oversight list, and the OTA, for programs not on the OSD T&E oversight list, shall determine*

the number of production or production-representative test articles required for IOT&E. To efficiently resource OT&E requirements, the OTA shall plan to leverage all operationally relevant T&E data and provide the PM with an early projection as to OT&E scope and resource requirements. See reference (b), enclosure 5, for implementation requirements for DON ACAT programs.]

IOT&E is defined as dedicated operational test and evaluation conducted on production, or production representative articles, to determine whether systems are operationally effective and suitable, and which supports the decision to proceed beyond low-rate initial production (LRIP). (Defined in Defense Acquisition University Glossary of Terms that can be located at https://akss.dau.mil/jsp/glossary.pdf)

Traditionally, Navy programs identified this phase of OT&E as OPEVAL.

OT&E is covered in this guidebook, enclosure (5), paragraph 5.7.

5.4.2.3 Software Intensive Systems

[***fm SNI 5000.2D, 5.4.2.3: The OTAs are encouraged to use DOT&E and CNO (N091) best practice guidance for testing software intensive system increments (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) and Major Automated Information System (MAIS) systems) in evolutionary acquisition. Although the process is discretionary, it effectively defines the scope and level of testing based on potential risk to mission areas, overall system complexity, and the complexity of changes in functionality within each increment.***]

This best practice decision process for software intensive systems is described in this guidebook, paragraph 5.7.2.2.5 and associated Annexes 5-F, 5-G, and 5-H.

5.4.2.4 T&E of Ships

Criteria for configuration, functionality, and engineering changes to the basic ship profile should be defined in the TES for a ship program. These criteria should be used to determine level and scope of T&E required for increments of the lead ship as well as follow ships. Approval of the TES and subsequent TEMPs should establish T&E requirements for ship and ship systems increments. Should the T&E WIPT not resolve issues, a TECG chaired by CNO (N091) will determine when a new ship, ship system or increment requires full ship OT&E.

DT&E and OT&E prior to Milestone B should normally address T&E of individual, new, or modified shipboard systems.

Individual weapon system's T&E should utilize land-based test sites (LBTSs) to the greatest extent possible. For prototype or lead ship acquisition programs, T&E should be conducted on the prototype or lead ship as well as on individual systems.

5.4.2.4.1 Ship Programs Without New Development

For ship programs not requiring OT&E, TEMP requirements may be satisfied by performance standards within the shipyard test program, as well as builder's trials, acceptance trials, and final contract trials, specified in the contract and in specifications invoked on the shipbuilder. Representatives of the cognizant PEO/DRPM or Naval Sea Systems Command (NAVSEASYSCOM) shipbuilding program office, the Supervisor of Shipbuilding for the respective shipyard, and the Board of Inspection and Survey (INSURV) normally observe the foregoing trials.

5.4.2.5 T&E of Space Systems

As stated in paragraph 5.2.3 of SECNAVINST 5000.2D, Space systems are exempt from T&E requirements contained herein. Policy and approach for T&E of Space Systems is contained in National Security Space Acquisition Policy 03-01, 27 Dec 04.

5.4.3 Test and Evaluation Working Integrated Product Team (T&E WIPT)

[***fm SNI 5000.2D, 5.4.3: Formerly referred to as a Test Planning Working Group (TPWG), the T&E WIPT is a DoD wide accepted forum for representatives from across program disciplines and oversight agencies to discuss, coordinate, and resolve test planning goals and issues. Within DON the T&E WIPT is the accepted forum for the PM to develop the TES and TEMP.***

The PM, or designated representative (normally military O-6/O-5 or civilian equivalent), is responsible for initiating and chairing the T&E WIPT.]

All participants in a T&E WIPT should be familiar with the USD (AT&L) publication, *Rules of the Road: A Guide for Leading Successful Integrated Product Teams*, that may be found at: https://acc.dau.mil/CommunityBrowser.aspx?id=24459

The following composition, responsibilities, and practices comprise the general business of a T&E WIPT:

1. Recommended membership:

   a. DA T&E IPT Lead is Chair

   b. Sponsor Requirements Officer (RO)

   c. OPNAV T&E (N091) Action Officer

d. OPNAV Readiness (N4) Action Officer

e. OPNAV Manpower (N1) Action Officer

f. OPNAV Education and Training (N12) Action Officer

g. OTA Operational Test Coordinator(s) (OTC) and the Operational Test Director(s) (OTD)

h. SYSCOM T&E representative(s)

i. Program Office DT&E representative(s)

j. Contractor T&E representative(s)

k. ONI Threat Analysis representative(s)

l. Representative(s) from certifying agencies (e.g. JITC, WSESRB, NTAB, etc.) as appropriate

m. Program Executive Office (PEO) representative

n. ASN(RD&A), appropriate DASN representative

o. DOT&E representative(s) when on OSD T&E oversight list

p. The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L))(DT&E) representative(s) when on OSD T&E oversight list

q. Test laboratories, facilities, and engineering subject matter expertise as needed.

r. Principal for Safety and ESOH Manager representatives.

2. Based on the acquisition strategy and the program’s proposed test strategy and concepts, the T&E WIPT should support the PM through review and discussion that offers subject matter expertise and policy guidance that seeks the most economical and effective T&E strategy and plans. Representatives should have sound subject matter expertise and authority to speak for their agency.

3. A T&E WIPT should be formed in the early Concept Refinement phase to begin a review of T&E strategy and lay plans for fully integrating the T&E effort.

4. Meeting agenda, minutes, and draft TEMPs should be maintained and distributed to all members as early as possible. Establishment of web-based forums is highly recommended. T&E WIPT leaders should be aware that key policy representatives are routinely members of several dozen, and in some cases hundreds, of programs, so it is essential to manage meeting schedules and distribution of information in forums that keep everyone well informed.

5. Sub-groups should be considered for various test phases and action items to keep subject matter expertise and agenda focused. All minutes and draft documents from these groups should be distributed to the membership. Sub-groups should be referred to as Test Plan Working Groups (TPWGs) for specific phase or action to efficiently direct communication and documentation.

5.4.4 Navy Test and Evaluation Coordination Group (TECG)

[***fm SNI 5000.2D, 5.4.4: When T&E issues arise that cannot be resolved by the T&E WIPT, a TECG should be convened. A TECG may also be used to implement urgent required changes to the TEMP. When used for urgent TEMP changes either a page change should be issued or the formal report of the TECG should be attached to the TEMP as an annex until the next required update or revision. When an activity determines a more formal solution is required to resolve an issue, the activity - via formal correspondence - will request that CNO (N091), as the responsible authority for T&E issue resolution, convene a TECG. For programs on the OSD T&E Oversight List, the TECG chair (CNO (N091)) shall coordinate results with DOT&E and USD(AT&L).***]

5.4.4.1 TECG Membership

When T&E issues require resolution, CNO (N912) coordinates the appropriate level of chair authority and convenes the TECG via formal correspondence with membership from:

1. CNO (N091) or (N912) Director Test and Evaluation Division - Chair

2. CNO (N912) T&E Staff Action Officer

3. Sponsor Requirements Officer (User Representative)

4. Program Manager

5. OPTEVFOR Assistant Chief of Staff (ACOS) for the particular warfare division

6. Applicable ASN(RD&A) program staff

7. ASN(RD&A) CHSENG representative when applicable

8. Supporting Subject Matter Experts to present issues and provide technical expertise. Agencies should submit attendance requests to CNO (N912) for these attendees and their purpose.

9. Others as appropriate

a. CNO (N4)

b. CNO (N1)

c. CNO (N12)

d. T&E WIPT members as required

5.4.4.2 Distribution of TECG Results

The results of the TECG should be reported in formal correspondence to all attendees with information copies distributed to all T&E WIPT membership.

5.4.4.3 TECG for a Consolidated Cryptologic Program (CCP)

The National Security Agency (NSA) has primary responsibility for developing and testing Consolidated Cryptologic Program (CCP) systems. A CCP TECG should be used to identify Navy-unique effectiveness and suitability issues for emergency CCP Programs, develop a coordinated Navy position on cryptologic T&E issues, and determine the extent of Navy participation in multi-service testing. A CCP TECG may also be used to resolve issues relating to assigning or canceling a CCP TEIN.

5.4.5 T&E Funding Responsibility

5.4.5.1 Developing Activity Responsibilities

[***fm SNI 5000.2D, 5.4.5.1: Except as noted below, the DA shall plan, program, budget, and fund all resources identified in the approved TEMP, to include the early OT involvement costs. Funds for OT&E should be transferred to the OTA for distribution as required. All T&E operating costs for OT squadrons (VX-1, VX-9, HMX-1) will be provided on a reimbursable basis by the DA to COMOPTEVFOR headquarters. The DA should not be required to fund:***

1. Fleet operating costs for RDT&E support,

2. Fleet travel for training,

3. Non-program-related OTA travel and administrative costs,

4. Non-program-related INSURV travel and administrative costs, and

5. Major Range and Test Facility Base (MRTFB) institutional costs.]

5.4.5.2 <u>Fleet Commanders Responsibilities</u>

[***fm SNI 5000.2D, 5.4.5.2: Fleet Commanders should plan, program, budget, and fund fleet travel for training, operating costs for RDT&E support provided by fleet units, and all costs associated with routine operational expenses except procurement costs of the systems tested and COMOPTEVFOR costs.***]

5.4.5.3 <u>Board of Inspection and Survey (INSURV) Responsibilities</u>

[***fm SNI 5000.2D, 5.4.5.3: INSURV should plan, program, budget, and fund INSURV travel costs and costs not related to programs under test.***]

5.4.5.4 <u>Non-Acquisition Programs Responsibilities</u>

[***fm SNI 5000.2D, 5.4.5.4: The Research and Development (R&D) agency for a non-ACAT or pre-ACAT program has responsibilities equivalent to those of the DA for T&E costs.***]

5.4.6 <u>Research, Development, Test and Evaluation (RDT&E) Support Provided by Fleet Commanders</u>

[***fm SNI 5000.2D, 5.4.6: A developing agency, PM, COMOPTEVFOR, INSURV, or R&D agency shall request support from Fleet Commanders for the accomplishment of T&E that is documented in a TEMP or other approved test document via CNO (N091/N912). A request should normally be initiated nine (9) months prior to test event.***]

Three levels of RDT&E support are as follows:

1. Dedicated support - precludes employment of the supporting unit(s) in other missions,

2. Concurrent support - permits employment of the supporting unit(s) in activities other than RDT&E support, but could have an operational impact upon unit employment, and

3. Not-to-interfere basis (NIB) support - permits RDT&E operational employment of the supporting unit(s) without significant interference with primary mission accomplishment.

5.4.6.1 Scheduling RDT&E Fleet Support

To ensure T&E support services are addressed in fleet employment scheduling conferences, requests will be submitted and updated on a quarterly basis beginning nine months prior to the quarter in which services are needed. Program Executive Officers (PEOs), SYSCOMs, and Direct Reporting Program Managers (DRPMs) should request DT&E services and COMOPTEVFOR should request OT&E services via formats in this guidebook, enclosure (5), Annex 5-B, using the procedures in paragraph 5.4.6.1.1. below. Immediately notify CNO (N091/N912) of any support cancellations.

5.4.6.1.1 Requests

Requests may be via message, correspondence, or email and should provide the following information as formatted in Annex 5-B.

1. Requests should be tailored to allow schedulers the greatest degree of flexibility.

2. Include a list of platforms (i.e. ships, aircraft, etc.) that have the correct equipment configuration installed to support the tests.

3. Designate unique fleet personnel support requirements (e.g.: SEAL Teams, ULQ13 Van/Crew).

4. Service request remarks: State time required to install and remove equipment and by whom. Address the following questions:

a. Can it be installed in an operational environment (i.e. pier-side for ships, flight-line for aircraft, etc.) or must the unit be inducted into a special facility (drydock, SRA, Depot, contractor site, etc.)?

b. What is the status of equipment certifications (e.g., Electromagnetic Compatibility (EMC), DD Form 1494, Defense Information Technology Security Certification and Accreditation Process (DITSCAP), JITC, Safety) and has the equipment installation been approved? By whom?

c. Will installation affect unit operation or other equipment onboard?

d. Is any crew training required? How many riders are required to embark (keep to a minimum)?

e. If more than one unit is required, state which units must work together and the minimum concurrent time.

5. Address impact on program if services are not filled such as:

a. Loss of programmed monies (specify amount).

b. Increased cost due to delay (specify amount).

c. Impact on related joint programs or operations.

d. Congressional and or/OSD interest or direction.

e. Unique factors:

(1) Deployment schedule of test asset.

(2) Overhaul schedule.

(3) "One-of-a-kind" underway events required for testing.

f. Delay in projected production and cost to Navy.

6. Requests go to: CNO WASHINGTON DC//N912/(appropriate OPNAV sponsor N-code), with information copy to COMOPTEVFOR NORFOLK VA//01B5/01B6//60P4.

5.4.6.1.2 <u>Fleet Support Priorities</u>

CNO (N091) assigns a fleet support priority relative to the urgency of maintaining the RDT&E schedule, as defined below, to all RDT&E support programs in the quarterly RDT&E support requirements. COMOPTEVFOR collects support requirements and coordinates with CNO (N091) for assignment of priorities.

1. Priority ONE - support takes precedence over normal fleet operations. RDT&E support requiring the degree of urgency to assign a priority ONE should be requested in writing by the program sponsor, without delegation. This request should contain justifying information including:

a. The next program decision point and its date,

b. The decision forum,

c. The impact should the program decision point slip, and

d. The date of the latest approved TEMP.

2. Priority TWO - support takes precedence within normal fleet operations.

3. Priority THREE - normal fleet operations take

precedence over support.

5.4.6.2 Unscheduled RDT&E Support Requirements

RDT&E support requests after the 9-month deadline (paragraph 5.4.6.1) will be submitted to CNO (N091/N912) and the program/resource sponsor with information copies to the Fleet Commanders and commands involved via message that complies with the format provided in Annex 5-B.

In addition to the procedures described in paragraph 5.4.6.1.1 above, the following steps should be taken.

1. Coordinate justification with sponsor that the event cannot be moved to the next quarter.

2. Coordination with all units supporting the event in the emergent timeframe being requested.

3. Coordinate request via phone conversation with CNO N912 Action Officer.

4. Send a message with the following subject line: SUBJ/EMERGENT (qtr) QUARTER FY (yr) SUPPORT REQUEST FOR CNO PROJECT (T&E identification number)//

5. Send the message TO CNO WASHINGTON DC//N912/(appropriate OPNAV sponsor's N-code)// and INFO the appropriate scheduling commands, units whose services are needed, and COMOPTEVFOR. CNO N912 needs official OPNAV sponsor concurrence before authorizing an emergent request.

5.4.6.3 RDT&E Fleet-Support Scheduling Agent

COMOPTEVFOR is designated the RDT&E fleet-support scheduling agent for CNO (N091).

5.4.6.4 Conduct of At-Sea T&E

COMOPTEVFOR, or designated representative, is responsible for the conduct of at-sea OT&E. The DA is responsible for the conduct of at-sea DT&E.

5.4.7 Test and Evaluation Master Plan (TEMP)

[***fm SNI 5000.2D, 5.4.7: All DON ACAT programs shall implement a TEMP for all developmental, operational, and live-fire testing in compliance with reference (b), enclosure 5. The TEMP may be a stand-alone document or it may be included as the T&E management portion of a Single Acquisition Management Plan (SAMP). If the TEMP is included in the SAMP, that T&E section must undergo the normal TEMP approval process. Although the TEMP format is discretionary, deviations from the standard DOT&E***

policy require concurrence from the TEMP approval authority. The TEMP for all ACAT programs shall specify entry criteria and resources required for each phase of testing. The TEMP shall identify anticipated use of M&S and the M&S proponent's verification, validation and accreditation (VV&A) strategy per reference (c). The TEMP documents the commitment between signatories to test events, schedules, and resources.

To meet Milestones B and C and Full-Rate Production Decision Reviews (FRP DRs), the PM for MDAPs, MAIS programs, and programs on the OSD T&E Oversight List shall submit the TEMP via concurrence of primary DON stake-holders, CNO (N091), and ASN(RD&A) to the USD(AT&L) and the DOT&E sufficiently early to satisfy review timelines designated by those agencies. TEMPS for ACAT II programs shall be approved by ASN(RD&A). The MDA for all other ACAT TEMPs shall have final approval authority. CNO (N091) is the OPNAV single point of contact for TEMP coordination with OSD. The DA is responsible for distribution of an approved TEMP to all agencies involved in testing, providing support or resources, oversight, or that have a relevant and official need to access testing information.]

See Annex 5-A of this enclosure for the signature authorities associated with the appropriate level of an ACAT program.

5.4.7.1 <u>Milestone B TEMP Approval for IT Systems, including NSS, and Spectrum Dependent Systems</u>

[***fm SNI 5000.2D, 5.4.7.1: National Security Systems (NSS), IT systems, and systems with Service and joint interoperability requirements, and/or systems that require use of the electromagnetic spectrum must comply with DOD and JCS Integrated Architecture Guidance. The following integrated architecture related items must be specifically addressed in Milestone B TEMP:***

1. Appropriate Net-Ready (NR) Key Performance Parameter (KPP) products for IT, including NSS, programs per reference (d),

2. Information Assurance Mission Assurance Category (MAC) and Confidentiality Level per reference (e),

3. Security Certification and Accreditation Phase 1 System Security Authorization Agreement (SSAA) or equivalent per references (f) and (g), and

4. Spectrum Certification Documentation: Stage 3 DD-1494 or Note to Holders per references (b) and (g). As an alternative, the MDA may grant authorization to proceed into System Development and Demonstration (SDD) Phase if, per reference (g), justification and a plan to achieve spectrum supportability has been provided to USD(AT&L), Assistant Secretary of Defense for Networks and Information Integration

(ASD(NII))/DoD Chief Information Officer (CIO), DOT&E, and the Chair, Military Communications-Electronics Board (MCEB).]

5. Include system E3 status and testing schedule to ensure compliance with reference (h) requirements.

5.4.7.2 <u>Milestone C TEMP Approval for IT Systems, including NSS, and Spectrum Dependent Systems</u>

[***fm SNI 5000.2D, 5.4.7.2: As systems mature during the development process, more detailed information becomes available. The following integrated architecture related items must be specifically addressed in Milestone C and beyond test phases:***

1. Information Assurance MAC, and Confidentiality Level, and related IA controls per reference (e),

2. Security Certification and Accreditation Phase 2 SSAA or equivalent per references (f) and (g),

3. Security Certification and Accreditation Interim Authority to Test (IATT)/Interim Authority to Operate (IATO) per references (f) and (g),

4. Appropriate NR KPP for IT, including NSS, programs per reference (d),

5. JITC assessment of interoperability readiness for an OT phase or the Interoperability Certification and Evaluation Plan (ICEP) is in place per reference (d),

6. E3 Verification/Validation reports/documentation per reference (h), and

7. Spectrum Certification Development: Stage 4 DD-1494 or Note to Holders per references (b) and (g). As an alternative, either USD(AT&L) may grant authorization to proceed into Production and Deployment Phase or ASD(NII) may grant a waiver if, per reference (g), justification and a plan to achieve spectrum supportability has been provided to USD(AT&L), ASD(NII)/DoD CIO, DOT&E, and the Chair, MCEB.]

5.4.7.3 <u>Capabilities, Key System Attributes (KSAs), and Key Performance Parameters (KPPs) Traceability to Critical Operational Issues (COI)

[***fm SNI 5000.2D, 5.4.7.3: For DON programs, traceability will be consistent among the analysis of alternatives, ICD/CDD/CPDs, acquisition program baseline (APB), and the***

TEMP. The TEMP shall document how specific capabilities, KSAs, and KPPs trace to COIs and how each will be addressed in T&E.

As described in enclosure (2), section 2.1.2.3 of this instruction, KSAs are system or sub-system capabilities with priority to Navy leadership for cost, schedule or performance insight, but do not meet criteria as KPPs. KPPs are those capabilities that leadership considers of such significance that if not demonstrated are reason for program reassessment or possible termination.]

5.4.7.4 <u>Performance Thresholds and Critical Technical Parameters (CTPs)</u>

[***fm SNI 5000.2D, 5.4.7.4: Testable and measurable performance thresholds for DT, LFT&E, and OT shall be established. The CTPs, derived from the capabilities documents shall be established and incorporated in the TEMP by the PM. The operational parameters and critical issues derived from the ICD/CDD/CPD to be used for OT shall be established and incorporated in the TEMP by COMOPTEVFOR/Director, MCOTEA. The numerical values for DT and OT shall be the same as the performance parameters established in the CDD/CPD. See reference (b), enclosure 5, for implementation requirements for all DON ACAT programs.***]

5.4.7.5 <u>Test Planning for Commercial and Non-Developmental Items</u>

[***fm SNI 5000.2D, 5.4.7.5: Use of commercial products built to non-DoD specifications dictates the need for the PM and the T&E community to be cognizant of the commercial T&E data, standards, and methods used to provide assurance for these products. In some cases, commercial T&E data or use of commercial T&E practices by the DoD T&E community may provide adequate, reliable, and verifiable information to meet specific DT&E, OT&E, or LFT&E goals. When it can be shown that commercially available T&E data or use of commercial T&E practices meet specific DoD T&E needs and costs less than their DoD T&E counterpart, they should be considered by the PM or the OTA, and may be used to support T&E requirements.***]

T&E of commercial and non-developmental items is required to ensure that the item will perform its intended military application. The PM or OTA, in the development of a TEMP, will assess the benefits and risks associated with T&E of commercial and non-developmental items and what verifiable information meets specific DT&E, OT&E, or LFT&E goals (to assume effective performance in the intended operational environment).

5.4.7.6 Use of Existing T&E Infrastructure

[*fm SNI 5000.2D, 5.4.7.6: Planners shall use existing investment in DoD ranges, facilities, and other DoD resources, to include embedded instrumentation for conduct of T&E unless it is demonstrated that the required capability does not exist within DoD or it is more cost effective to use a non-DoD resource. Projected T&E investment needs will be annotated in the TEMP (normally Part V). Infrastructure shortfalls that adversely impact the conduct of a specific T&E requirement will be identified in Limitations to Test in the TEMP.*]

5.4.7.7 Environmental Protection

[*fm SNI 5000.2D, 5.4.7.7: Prior to any live fire, developmental or operational test decision that may affect the physical environment, the PM, per references (i) and (j), shall satisfy all applicable National Environmental Policy Act (NEPA)/Executive Order (EO) 12114 requirements. Testing shall be planned to ensure sufficient time to comply with applicable environmental requirements including NEPA and EO 12114. Environmental impact considerations that directly affect testing shall be addressed in the TEMP and respective test plans as limitations or conditions of the testing. Test activities that may require NEPA/EO 12114 analyses shall be identified in the NEPA/EO 12114 Compliance Schedule, which is required as part of the Program's Programmatic Environment, Safety and Occupational Health Evaluation (PESHE) and Acquisition Strategy. See reference (b), enclosure 7, paragraph E7.7, and reference (k) for implementation requirements for all DON ACAT programs.*]

See reference (l) for guidance in minimizing the impact on the environment. Requirements for environmentally compliant facilities, tools, and methods should be identified early by the DA and OTA to allow for funding and development. The results of these requirements should be outlined in the programmatic environmental, safety, and occupational health evaluation. Those aspects, which directly affect testing, should be addressed in the TEMP as limitations or conditions of the testing.

5.4.7.7.1 Environmental, Safety and Occupational Health (ESOH)

Systems acquisition policy requires ESOH regulatory compliance and risk management throughout the acquisition process. To provide essential information to decision makers, the T&E Strategy and TEMP should assess the PM's acceptance of residual ESOH risks and control measures, to include safety releases, for the system or item. The intent is to ensure that, prior to OT&E and fielding, the testers and users understand the ESOH hazards, the control measures adopted by the PM, and the residual risks accepted by the PM. Early participation of ESOH

expertise on the T&E WIPT is recommended to assure appropriate issues are addressed during test planning and execution. Additionally, T&E planning should consider testing for specific system characteristics that may have an environmental or personnel safety and health impact (e.g. air emissions, noise, liquids/effluent characterization).

5.4.7.7.2 Responsibilities for Environmental Compliance During Testing

The PM is responsible for compliance with National Environmental Policy Act (NEPA)/E.O 12114 requirements, particularly as they affect test ranges and operational areas. The Testing Strategy and TEMP should include NEPA/E.O.12114 documentation requirements, and describe how analyses will be conducted to support test site selection decisions.

COMOPTEVFOR or Director, MCOTEA, or designees, are action proponents for dedicated OT&E. See enclosure (7) of this guidebook, paragraph 7.3.2, National Environmental Policy Act and E.O. 12114 Environmental Effects Abroad, for action proponents' responsibilities.

5.4.7.7.3 Safety Releases for Testing

Reference (b), enclosure 6, paragraph 1b, requires the PM to provide safety releases to developmental and operational testers prior to any test using personnel. A Safety Release communicates, to the activity or personnel performing the test, the risks associated with the test and the mitigating factors required to safely complete the test. A secondary function of the process is to ensure that due diligence is practiced with respect to safety in the preparation of the test by the sponsor. A Safety Release is normally provided by the PM after appropriate hazard analysis. Safe test planning includes analysis of the safety release related to test procedures, equipment, and training.

5.4.7.8 Operational Test and Evaluation (OT&E) for Non-acquisition Programs

[***fm SNI 5000.2D, 5.4.7.8: OTA services may be required to evaluate capabilities of non-acquisition programs or pre-systems acquisition equipment or programs. At a minimum, the requesting agency must provide a statement describing mission functions with thresholds for any capabilities of interest. A test plan must be approved by the OTA prior to any OT.***]

5.4.7.9 Modeling and Simulation (M&S)

[***fm SNI 5000.2D, 5.4.7.9: Per reference (b), enclosure 5, M&S may be used during T&E of an ACAT program to represent conceptual systems that do not exist and existing systems that***

cannot be subjected to actual environments because of safety requirements or the limitations of resources and facilities. M&S applications include hardware/software/operator-in-the-loop simulators, land based test facilities, threat system simulators, C4I systems integration environments/facilities and other simulations as needed. M&S shall not replace the need for OT&E and will not be the primary evaluation methodology. M&S shall not be the only method of meeting independent OT&E for beyond LRIP decisions per Title 10 U.S.C. Section 2366. M&S is a valid T&E tool that per reference (c) requires VV&A to supplement or augment live test data. The PM is responsible for verification and validation (V&V) of M&S and the accreditation of M&S used for DT&E. The OTA is responsible for accreditation of M&S used for OT&E. The PM is required to complete V&V prior to an accreditation decision by the OTA. M&S previously accredited for other programs or test phases requires accreditation for specific use by the OTA for each OT&E. Use of M&S shall be identified in the TEMP for each DT&E and OT&E phase it is intended to support (normally Parts III and IV respectively). M&S required resources shall be listed in the TEMP (normally Part V).]

Examples of M&S that may be used for DT&E and OT&E include:

1. to assess the adequacy of future test plans,

2. to assess performance against threats that there is not a real system to test against,

3. to adequately test complex systems in dense combat environments,

4. to conduct pre-test predictions of system performance, and

5. to augment live test data in assessing KPPs, CTPs, and MOPs.

[***fm SNI 5000.2D, 5.4.7.9: The PM shall identify and fund required M&S resources early in the acquisition life cycle. The T&E WIPT shall develop and document a robust, comprehensive, and detailed evaluation strategy for the TEMP, using both simulation and test resources, as appropriate. See reference (b), enclosure 5, for implementation requirements for all DON ACAT programs.***]

5.4.7.10 <u>Interoperability Testing and Certification</u>

[***fm SNI 5000.2D, 5.4.7.10: The OTA has a responsibility to evaluate progress towards joint interoperability as part of each testing phase. Interoperability testing consists of intra-Service Navy-Marine Corps, joint Service, and where applicable, allied and coalition testing. Interoperability requirements are covered in detail by references (d), (m), and (n). Systems designated***

for FORCEnet compliance must achieve joint interoperability test certification. Testing for FORCEnet compliance will be in conjunction with DT and OT to the maximum extent possible. Lab environments used to conduct live, constructive, and virtual interface and interoperability testing must be verified, validated, and accredited by the PM and OTA per reference (c). See reference (b) for implementation requirements for DON ACAT programs. The following general procedures apply to IT systems, including NSS:

1. Interoperability capabilities (requirements) will be documented in the ICD, CDD, and CPD. The PM is responsible for developing Information Support Plan (ISP) for IT, including NSS, programs based upon documented requirements.

2. Marine Corps-unique interfaces shall be tested during DT&E by MARCORSYSCOM, typically at Marine Corp Tactical Systems Support Activity (MCTSSA).

3. Navy-unique interfaces shall be tested during DT&E by DAs (e.g., PEO-C4I and PEO-EIS).

4. DON PMs will coordinate with JITC to develop and execute interoperability testing for certification of IT, including NSS, programs per reference (d). When appropriate, for complex IT systems, including NSS, the PM shall obtain an Interoperability Certification Evaluation Plan (ICEP) from JITC.

5. Navy systems processing data links (e.g., Link 4/11/16/22) and character oriented message for human readable text (e.g., USMTF and OTH-Gold), must be tested for joint interoperability by Naval Center for Tactical Systems Interoperability (NCTSI), and by JITC for Joint certification.

6. Marine Corps systems processing data links (e.g., Link 4/11/16/22) and character oriented message human readable text (e.g., USMTF and OTH-Gold) must be initially tested for joint interoperability by MCTSSA, then by JITC for Joint certification.

7. Standard conformance testing with interoperability certification of specific data link interfaces should be accomplished prior to IOT&E. Per reference (d), a Joint Interoperability Test Certification or an Interim Certification to Operate (ICTO) shall be accomplished prior to FRP DR.

8. Per references (b), (d), and (m) and SECNAVINST 5000.2D, Table E3T2, all IT, including NSS, ACAT programs are required to receive Joint Staff (J-6) interoperability and C4I

supportability certifications at FRP DR. This certification shall be used as the basis for certification of compliance with the applicable FORCEnet technical standards.]

5.4.7.10.1 <u>Joint Interoperability Process and Support</u>

Although Joint Interoperability Test Command (JITC) is the sole joint interoperability certifier in DoD per reference (d), certification test execution can be conducted by JITC or Program Manager (PM). The PM can either fund and task JITC for a separate certification test on all phases of test execution (e.g., test plan, test configuration and data collection and analysis) or leverage DT, exercises, and OT events as long as the test plan has JITC concurrence.

5.4.7.10.1.1 <u>Three Types of Joint Interoperability Test Command (JITC) Certification Reports</u>

1. Standards Conformance Certification: System is certified for conformance to a standard (e.g., UHF DAMA SATCOM, HF Radio MIL-STD, NATO STANAGs, etc). This certification is necessary but not sufficient in itself for fielding.

2. Full Certification: Full system certification. System meets "all" certified Net-Ready Requirements (NR-KPPs) and is ready for fielding.

3. Partial Certification: Partial system certification. System meets subset of the certified NR-KPPs and that part/version of the system is ready for fielding.

5.4.7.11 <u>Information Assurance (IA) and Information Systems Security Certification and Accreditation</u>

[***fm SNI 5000.2D, 5.4.7.11: IA is critical to Net- centric Warfare. The MAC and Confidentiality Level, as approved by the Deputy CIO for the Navy or Marine Corps, establish IA control measures that must be incorporated into a system. Control measures are implemented, verified and validated via Security Certification and Accreditation (SCA). Reference (e) also requires V&V of control measures through vulnerability assessments and penetration testing. The Defense Information Technology Security Certification and Accreditation Process (DITSCAP) is the most common methodology used to V&V information assurance control measures. The PM coordinates with the OTA, and the Designated Approving Authority (DAA) (CNO/CMC, or designee) to determine the extent of information systems security certification testing required. The PM documents SCA and IA controls in the TEMP, and the OTA reports on these controls as part of OT. An IATT or IATO must be obtained prior to OT. The OTA will evaluate IA controls and ability to detect, respond, and restore systems during OT based upon MAC and Confidentiality Level.***

The OTA does not certify the system for security or IA, but evaluates the effectiveness, suitability, and survivability of the system in its intended environment.]

5.4.7.12 <u>Anti-Tamper Verification and Validation Testing</u>

[***fm SNI 5000.2D, 5.4.7.12: Anti-Tamper (AT) Verification and Validation (V&V) is a requirement for all systems implementing an AT plan to ensure the AT techniques stated in the AT plan are fully implemented and respond appropriately in the event of tampering. This V&V must be accomplished by an independent team and be funded by the parent acquisition program. See reference (b) for implementation requirements for DON ACAT programs that contain critical program information and AT countermeasures. DON's AT Technical Agent (Office of Naval Research (ONR)), in support of DON's AT Technical Authority (NAVAIRSYSCOM), will assist acquisition programs in understanding AT V&V requirements, program test plan development, and interactions with the DoD V&V community.***] NAVAIRSYSCOM, in concert with DoD AT Executive Agent (Assistant Secretary of the Air Force for Acquisition), will assist the PM in designating the independent team to perform anti-tamper V&V testing.

Per reference (b), enclosure 2, paragraph 6, the purpose of the SDD phase includes ensuring the protection of information with techniques such as anti-tamper (AT).

The FRP decision should not be given favorable consideration until AT implementation is fully verified and validated during DT and OT, and ready for production.

Reference to the AT annex in the PPP may be adequate for TEMP documentation if test resource requirements can be properly identified in Part V of the TEMP. When necessary an appropriately classified AT annex to the TEMP may be required.

The intent of AT testing is to integrate testing within the events of routine DT and OT rather than requiring increased testing events. The conduct of V&V for anti-tamper (AT) requirements is best served with a multi-disciplined team of subject-matter experts. This system engineering process must consider protection of the system's mission and performance requirements. Programs are responsible for satisfactory V&V of their respective AT plan implementation prior to Milestone C, Foreign Military Sale, or Direct Commercial Sale decisions. DON AT Technical Agent (PMR-51) can assist acquisition programs in understanding AT V&V requirements, program V&V test plan development, and interactions with the DoD V&V community.

5.4.7.13 <u>Test and Evaluation Identification Number (TEIN) Assignment</u>

[***fm SNI 5000.2D, 5.4.7.13: A TEIN is required before requesting fleet support services. The TEIN assists in tracking T&E documentation, scheduling fleet services, and execution of oversight requirements. The PM shall request, in writing, a TEIN from CNO (N091) via the resource sponsor***.]

The recommended format for a TEIN request is provided in this guidebook, enclosure (5), Annex 5-C. CNO (N091) identifies six types of programs via a code letter preceding the number in a TEIN as follows:

1. DON ACAT programs (no code letter)

2. Tactics programs (Code "T")

3. Software Qualification Programs (Code "S")

4. OSD-Directed joint T&E programs (Code "J")

5. Non-acquisition programs (Code "K")

6. Foreign comparative testing (FCT) programs (Code "F"), only when fleet services will be required to support testing.

5.4.7.13.1 <u>Pre-requisite Documentation</u>

TEINs should not be assigned to programs that do not have approved documentation. Minimum documentation requirements are:

1. An approved ICD for ACAT programs,

2. A RDT&E Budget Item Justification Sheet (R-2 Exhibit) for non-acquisition programs,

3. Documentation as discussed in SECNAVINST 5000.2D, enclosure (2), paragraph 2.4.6, for Abbreviated Acquisition Programs, or

4. Designation as a Software Qualification Program.

By endorsement, the program sponsor should ensure the request for TEIN assignment is supported by valid documentation.

5.4.7.13.2 <u>Program Groups</u>

TEINs should be structured for generic project groups and subprojects. Generic project groups should be consolidated by identifying the basic project and functionally related sub-projects. If the project for which a TEIN is being requested

is a sub-project of an existing project group, it should be so noted and the generic project number should be included. Likewise, multiple TEINs may be requested in a single letter.

5.4.7.13.3 Consolidated Cryptologic Programs (CCP)

Assignment of CCP TEINs should be per the following procedures:

1. Commander Naval Security Group (COMNAVSECGRU) should review draft project baseline summary one (PBS-I) on new CCP programs.

2. If COMNAVSECGRU determines that the system has significant and continuous Navy tactical implications, the PBS-I will be sent to COMOPTEVFOR for review.

3. If COMOPTEVFOR concurs, COMNAVSECGRU should include the requirement for Navy operational testing in PBS-I comments to the National Security Agency and forward a recommendation for TEIN assignment to CNO (N912).

5.4.7.13.4 Inactive TEINs

CNO (N912) should, with DA and program sponsor review, cancel TEINs, which have been inactive in excess of 1 year and/or require no further testing.

5.4.7.14 TEMP Approval

A major function of the T&E WIPT is to resolve issues. Once issues are resolved to the satisfaction of an O-6 review for all ACAT I, II, and programs with OSD T&E oversight, the PM should submit the smooth TEMP to the DA (SYSCOM, PEO, DRPM) for concurrence and further routing. The DA should distribute copies of the smooth TEMP to all signature offices and coordinate the sequential routing of a smooth signature page to the OTA and program sponsor (user representative) for their concurrence. For Navy sponsored TEMPs with all concurrent signatures the DA should coordinate delivery of the TEMP signature page to CNO (N091) for Service component approval prior to forwarding to ASN(RD&A) for Component Acquisition Executive (CAE) approval. Marine Corps sponsors are authorized to forward Marine Corps TEMPs direct to ASN(RD&A). Use the cover page in this guidebook, enclosure (5), Annex 5-A, for ACAT I programs and all DON programs with OSD T&E oversight. TEMP signature routing for ACAT II, III, and IV programs should comply with the sample TEMP cover pages provided in this guidebook, enclosure (5), Annex 5-A. A separate Navy TEMP cover sheet format is provided for legacy software qualification testing.

5.4.7.14.1 TEMP Timing

A TEMP is to be submitted to OSD not later than 45 days prior to the milestone decision point or subsequent program initiation if a PM must have an OSD-approved document by the decision date. For programs newly added to the OSD T&E-oversight list, the TEMP must be submitted within 120 days of such written designation.

5.4.7.14.2 TEMP Drafting/Submitting

The PM/DA drafts the TEMP with T&E WIPT participation. The PM/DA should draft the LFT&E section of part IV of the TEMP. The OTA is responsible for drafting paragraph d of part I, part IV, and inputs to applicable sections of part V. ACAT IVT draft TEMPs should be sent to the applicable program sponsor for review and to the OTA for review and endorsement.

Requirements developed in the analysis of alternatives and incorporated in the increment under development in the CDD/CPD should be listed in the TEMP. Other increment requirements should be time-phased or put in TEMP annexes, as appropriate.

When the T&E WIPT membership considers the draft TEMP ready for approval, the PM/DA Lead should distribute copies of the draft TEMP to all members of the T&E WIPT, staff action offices for all TEMP signatories, and ASN(RD&A) CHSENG for O-6 level review and comment. All comments should be returned to the PM/DA T&E Lead for consolidation, consideration, and incorporation. The PM/DA should convene a T&E WIPT session to review the consolidated TEMP comments, with rationale and disposition of all recommended changes, and the final TEMP. All known issues should be resolved before submitting the TEMP for final approval. The PM/DA is responsible for sending copies of the TEMP and disposition of all O-6 level comments to all signature offices. If the program is subject to OSD T&E oversight, the DA should deliver appropriate copies to OSD per reference (b). For Navy sponsored programs, CNO (N091) is the single OPNAV point of contact with OSD for TEMP coordination.

5.4.7.15 TEMP Distribution

The DA distributes approved TEMPs to all appropriate offices and commands. Approved TEMPs for ACAT IVM programs should be sent to the applicable program sponsor and COMOPTEVFOR or Director, MCOTEA for information.

5.4.7.16 TEMP Updates

Within DON, TEMP updates (as described in DODI 5000.2) fall into two categories, revision and administrative change. A revision is signed by all TEMP signatories and is identified with a sequential alphabetic designation to the TEIN. An

administrative change may be promulgated by the program manager based on the concurrence of the T&E WIPT members who represent the signatories. An administrative change is identified with a sequential numeric designation to the TEIN.

5.4.7.16.1 TEMP Revision

A revision addresses changes to evaluation criteria, to scope of testing, to major resource changes, and/or to performance requirements. A revision may also be required if unanimous agreement is not reached to submit an update as an administrative change. Such a revision follows the approval chain for signature of principals at every level as detailed in the DON Acquisition and Capabilities Guidebook, Annex 5-A. The TEMP title includes "Revision" and a sequential alphabetic designation.

5.4.7.17 Administrative Change to TEMP

An administrative change reflects fact-of-life changes such as personnel, schedule, test status, history, etc. These changes are assessed as low risk for adversely impacting the scope of planned testing, milestones, or the Acquisition Program Baseline.

5.4.7.17.1 Determination on Administrative Change to a TEMP

Proposed administrative changes will be reviewed by the T&E WIPT. If each T&E WIPT member representing a signatory of the TEMP concurs, the program manager documents concurrence from each with the promulgation of the administrative change to the TEMP. If there is not complete agreement of those T&E WIPT members, the program manager may solicit more senior agreement from those dissenting organizations. In no case should there be untimely delay in beginning a revision cycle in order to solicit those more senior agreements. Navy programs soliciting Office of Secretary of Defense (OSD) for more senior agreements are represented by CNO (N091). USMC programs need Director, MCOTEA’s concurrence before soliciting OSD for more senior agreements. Navy programs not on OSD Test and Evaluation (T&E) Oversight may request that CNO (N091) facilitate discussions or convene a Test and Evaluation Coordination Group (TECG) in accordance with SECNAVINST 5000.2 series to resolve dissenting opinions concerning appropriate application of an administrative change for a TEMP update. No program should unduly delay (in no instance should a delay be over 30 days) beginning a revision cycle to obtain adjudication on the proposed administrative change. If the proposed changes are considered significant by a representative of a TEMP signatory, then the TEMP update would become a revision and handled accordingly.

5.4.7.17.2 Procedure for an Administrative Change to a TEMP

The program manager promulgates a TEMP change with a cover letter referencing the concurrences of the applicable T&E WIPT members and a short summary of the administrative changes to the TEMP. A TEMP change package is distributed to all TEMP holders. At a minimum, the TEMP Change package includes:

1. The cover letter.

2. A record of change pages.

3. Change bars in the right margin for all changes.

4. A notation indicating the TEIN number, version, and change number (e.g., TEMP XXXX Rev A CH-1) at the upper right corner on all pages containing changes. Changes are numbered consecutively by original or revision.

Programs on OSD T&E Oversight may require an approval letter from the oversight agencies authorizing the administrative change to the TEMP. A copy of the approval letter becomes part of the Program Manager's change package that is distributed to all TEMP holders.

5.5 Developmental Test and Evaluation (DT&E)

[***fm SNI 5000.2D, 5.5: The DA shall conduct adequate DT&E throughout the development cycle to support risk management, provide data on the progress of system development, and to determine readiness for OT. For DON programs, DT&E shall be conducted by the DA through contractor testing or government test and engineering activities. Developmental testing schedules require sufficient time to evaluate results before proceeding to independent OT phases. See reference (b), enclosure 5, for implementation requirements for all DON ACAT programs.***]

5.5.1 DT&E Data

[***fm SNI 5000.2D, 5.5.1: Data and findings from DT&E may be used by the OTA to supplement OT&E data. Within proprietary, contractual, and regulatory considerations all DT data shall be available to appropriate oversight agencies. Data will normally be made available upon completion of analysis by the primary analyzing agency. DT data and reports shall be available for review by the OTA with adequate time to finalize OT planning (normally 30 days prior to the commencement of OT). See reference (b), enclosure (5), for implementation requirements for all DON ACAT programs.***]

During combined DT/OT, DT data and reports will be handled

as specified by mutual agreement between the Lead Test Agency and the System Program Manager.

5.5.2 Information Assurance and Security Certification during Developmental Test (DT)

[***fm SNI 5000.2D, 5.5.2: IA testing and System Security Certification and Accreditation shall be conducted by the PM as part of the development process to ensure that appropriate control measures are in place to support the assigned MAC and Confidentiality Level. The MAC and Confidentiality Level should be identified in capabilities development documents and have approval of the Deputy CIO for the Navy/Marine Corps, as appropriate. Security Certification and Accreditation Testing shall be accomplished during DT by the PM in conjunction with the Security Certification and Accreditation Agent as approved by the DAA to ensure the appropriate combination of security controls and procedures have been implemented to achieve the required level of protection. per references (f) and (g), the DAA shall provide an accreditation statement prior to the FRP DR, Full-Rate Production and Deployment Approval. The PM shall coordinate with the security certification authority, the OTA, and the DAA to determine the extent of security certification testing required.***]

5.5.3 Production Qualification Test and Evaluation

[***fm SNI 5000.2D, 5.5.3: See reference (b), enclosure 5, for implementation requirements for all DON ACAT programs.***]

5.5.4 DT&E Phases and Procedures

DT&E should be conducted in three major phases to support Pre-Systems Acquisition, Systems Acquisition, and Sustainment phases of the acquisition model. The specific objectives of each phase should be developed by the DA and outlined in the TEMP. Modeling and simulation techniques, if used to assess areas in which testing is not yet possible or practical, as well as establishing and implementing software development metrics, requires proper validation (see OTRR certification criteria in SECNAVINST 5000.2D, paragraph 5.6.1). Annex 5-D depicts a notional schedule of DT phases within the phases of the Acquisition Model.

5.5.4.1 DT-A

DT-A is conducted during technology development to support Milestone B, if required.

5.5.4.2 DT-B/DT-C (TECHEVAL)

DT-B is conducted during system development and demonstration (SDD) to support the Milestone C decision. DT-C is conducted after Milestone C during low-rate initial production to

support the Full-Rate Production Decision Review. The last portion of DT-C prior to IOT&E may be designated TECHEVAL. This period is for rigorous technical testing at the end of development to demonstrate system stability, technical maturity, and to determine if the system is ready for IOT&E. DT-C/TECHEVAL should include, as a minimum, testing and assessment to determine:

1. System performance and verification of CTP compliance (including electronic countermeasures (ECM), electronic counter countermeasures (ECCM)),

2. System and personnel safety, occupational health hazards, the effects of volatile materials, effects of aging and environmental stress on energetic materials, and compliance with insensitive munitions criteria,

3. All electromagnetic environmental effects, such as: electromagnetic compatibility (EMC), electromagnetic interference (EMI), electromagnetic vulnerability (EMV), hazards of electromagnetic radiation to ordnance (HERO) and fuel (HERF), hazards of electromagnetic radiation (RADHAZ) to personnel (HERP), lightning, electrostatic discharge (ESD), and electromagnetic pulse (EMP),

4. The effectiveness and supportability of any built-in diagnostics, and

5. Compliance with FORCEnet and joint technical standards in the DoD Information Technology Standards Registry (DISR) that has replaced the joint technical architecture (JTA).

The OTA and the DA should determine what constitutes production representative hardware and what degree of software maturity (e.g., software requirements, software quality, computer resource utilization, build release content) is necessary for technical evaluation (TECHEVAL) data to be used in support of OT&E. Software to be used for IOT&E should be the same as or functionally representative of that software intended for fleet use at initial operational capability (IOC) of a system and will be validated during DT.

5.5.4.3 <u>DT-D</u>

DT-D is conducted during full-rate production and deployment and operations and support. Production acceptance test and evaluation (PAT&E) should be the responsibility of the DA. PAT&E objectives, excluding factory inspections and certifications, should be outlined in the TEMP.

5.5.4.4 <u>DT&E Schedules</u>

The DA should provide OTA with schedules of DT&E activities, program and system documentation (in draft form, if

necessary), and access to DT&E activities.

5.5.4.5 Operator and Maintenance Training

Prior to IOT&E, the DA is responsible for providing fleet/field representative system operator and maintenance training for the Operational Test Director (OTD) and members of the operational test team (including crew members, staffs, and interoperable units, when applicable). Scheduling of this training requires early coordination between OTA, the DA, and fleet/field units.

5.5.4.6 Live Fire Test and Evaluation (LFT&E)*

The DA is responsible for LFT&E per statute Title 10 U.S.C. Section 2366 and submission of the LFT&E section in Part IV of the TEMP. Paragraph 5.9 in enclosure (5) of this guidebook provides mandatory procedures and guidance on LFT&E.

*Not applicable to AIS programs

5.5.4.7 United States Marine Corps (USMC) Developmental Test and Evaluation

The USMC DT&E Handbook published 28 September 2000, provides detailed guidance for DT&E.

5.5.4.7.1 DT&E of Amphibious Vehicles

All DT&E of amphibious vehicles and amphibious tests of other equipment or systems used by a landing force in open seaways should be conducted by, or be under the direct supervision of, CG, MARCORSYSCOM with appropriate NAVSEASYSCOM or PEO/DRPM coordination. The Director, MCOTEA coordinates OT planning, scheduling, and evaluation of such systems with OPTEVFOR.

5.6 Certification of Readiness for Operational Testing

5.6.1 DON Criteria for Certification

[***fm SNI 5000.2D, 5.6.1: Per reference (b), the following list of criteria for certification of readiness apply to all IOT&E for all DON programs. For all OT other than IOT&E, the PM with the support of the T&E WIPT and concurrence of the OTA may tailor criteria listed below in sub items 2 through 20. The MDA may add criteria as necessary to determine readiness for OT.***

1. The TEMP is current and approved. Testing prior to Milestone B must have an approved TES as discussed in enclosure (5), paragraph 5.3.1.

2. Test and evaluation results indicate DT objectives and performance thresholds identified in the TEMP have been satisfied or are projected to meet system maturity for the ICD/CDD/CPD, as appropriate.

3. All significant areas of risk have been identified and corrected or mitigation plans are in place.

4. Test results have been provided to the OTA not less than 30 days prior to the commencement of OT, unless otherwise agreed to by the OTA.

5. Entrance Criteria for OT identified in the TEMP have been satisfied.

6. System operating, maintenance, and training documents have been provided to the OTA 30 days prior to the OTRR, unless otherwise agreed to by the OTA.

7. Logistic support, including spares, repair parts, and support/ground support equipment is available as documented. Discuss any logistics support which will be used during OT&E but will not be used with the system when fielded (e.g., contractor provided depot level maintenance).

8. The OT&E manning of the system is adequate in numbers, rates, ratings, and experience level to simulate normal operating conditions.

9. Training has been completed and representative of that planned for fleet units.

10. All resources required to execute OT including instrumentation, simulators, targets, expendables, and funding have been identified and are available.

11. Models, simulators, and targets have been accredited for intended use.

12. The system provided for OT&E, including software, is production representative. Differences between the system provided for test and production representative configuration must be addressed at the OTRR.

13. Threat information (e.g., threat system characteristics and performance, electronic countermeasures, force levels, scenarios, and tactics), to include security classification, required for OT&E is available to satisfy OTA test planning.

14. The system is safe to use as planned in the concept of employment and the PM has provided the appropriate safety release(s) for the phase of test to be conducted. Any

restrictions to safe employment are stated. The Environmental, Safety, and Occupational Health (ESOH) program requirements have been satisfied per references (i), (j), (k), (l), (o), (p), (q), (r), and (s). The system complies with Navy/Marine Corps ESOH/hazardous waste requirements, where applicable. ESOH/hazardous waste reviews and reports have been provided to COMOPTEVFOR or Director, MCOTEA. When an energetic is employed in the system, WSESRB criteria for conduct of test have been met.

15. All software is sufficiently mature and stable for fleet introduction. All software Trouble Reports are documented with appropriate impact analyses. There are no outstanding Trouble Reports that:

a. Prevent the accomplishment of an essential capability,

b. Jeopardize safety, security, or other requirements designated "critical,"

c. Adversely affect the accomplishment of an essential capability and no work-around solution is known, or

d. Adversely affect technical, cost, or schedule risks to the project or to life-cycle support of the system, and no work-around solution is known.

16. For software qualification testing (SQT), a Statement of Functionality that describes the software capability has been provided to COMOPTEVFOR and CNO (N091). For programs to be tested by MCOTEA, the SQT Statement of Functionality has been provided to Director, MCOTEA.

17. For aviation programs, there are no uncorrected NAVAIRSYSCOM deficiencies that affect:

a. Airworthiness,

b. Capability to accomplish the primary or secondary mission,

c. Safety of the crew/operator/maintainer,

d. Integrity of an essential subsystem,

e. Effectiveness of the operator or an essential subsystem,

18. For a program with interoperability requirements (e.g., information exchange requirements in ICD/CDD/CPDs), appropriate authority has approved the ISP and JITC concurs that program interoperability has progressed sufficiently for the phase of OT to be conducted.

19. For spectrum management per reference (g), a Stage 3 "Developmental" DD-1494 (at a minimum) is required for testing.

20. For IT systems, including NSS, the system has been assigned a MAC and Confidentiality Level. System certification accreditation documents, including the Phase 2 SSAA and the IATT, or IATO, or platform IT designation letter, as applicable, have been provided to the OTA.]

Note to item #14: PM is responsible for providing a Safety Release for any tests that involve personnel.

5.6.2 <u>Navy Procedures for Certification</u>

[***fm SNI 5000.2D, 5.6.2: The SYSCOM Commander/PEO/DRPM/PM shall convene an OTRR prior to certifying readiness for IOT&E per reference (b). The need to conduct and the procedures for an OTRR for all OT other than IOT&E shall be determined by the SYSCOM Commander/PEO/DPRM/PM with the concurrence of the OTA and based on recommendations from the T&E WIPT. An OTRR shall consist of those members of the testing team who provide input to the certification criteria, and representatives from CNO (N091), the program sponsor, ASN(RD&A) Chief Engineer (CHSENG), and COMOPTEVFOR. For programs on OSD T&E Oversight, representatives from OUSD(AT&L) and DOT&E shall be included.***

The SYSCOM Commander/PEO/DRPM shall evaluate and make a determination that a system is ready for OT&E (normally 30 days prior to OT&E). The SYSCOM Commander/PEO/DRPM shall, unless otherwise directed by ASN(RD&A) for programs on the OSD T&E oversight list make one of the following certifications.

5.6.2.1 <u>Certification for OT Without T&E Exceptions</u>

Certify to COMOPTEVFOR by message that a system is ready for OT_____(phase), as required by the TEMP, without deferrals or waivers. Provide information copies to CNO (N091), the program sponsor, ASN(RD&A) CHSENG, fleet commands, INSURV for ships, NTAB for aircraft, other interested commands, and when a program is on the OSD T&E Oversight List, to DOT&E. See this enclosure, paragraph 5.6.4 for explanation of exceptions.

5.6.2.2 <u>Certification for OT With T&E Exceptions</u>

Certify to CNO (N091) by message that a system is ready for OT_____(phase), as required by the TEMP, with waiver and/or deferral requests. Provide information copies to the program sponsor (who must provide formal concurrence with proposed exceptions), ASN(RD&A) CHSENG, COMOPTEVFOR, and when a program is on the OSD T&E Oversight List, to DOT&E.]

5.6.3 Marine Corps Procedures for Certification

[*fm SNI 5000.2D, 5.6.3: Approximately 30 days prior to the start of an OT&E, an OTRR will be chaired and conducted by the Director, MCOTEA. OTRR participants shall include the OT&E Test Director and Assistant Test Director, representatives from the PM, ASN(RD&A) (for ACAT I and II programs), MARCORSYSCOM Assistant Commander, Programs and Chief Engineer, and Marine Corps Combat Development Command (MCCDC) (CD&I Division). The purpose of the OTRR is to determine the readiness of a system, support packages, instrumentation, test planning, and test participants to support the OT. It shall identify any problems which may impact the start or proper execution of the OT, and make any required changes to test plans, resources, training, or equipment.*

CG, MARCORSYSCOM or Deputy Commander shall, unless otherwise directed by ASN(RD&A) for programs on the OSD T&E oversight list, certify to the Director, MCOTEA, that the system is safe and ready for operational testing. This certification includes an information copy for MCCDC (CD&I Division).

Director, MCOTEA, shall select OTRR agenda issues based on a review of DT&E results and related program documentation, including certification of equipment to be safe and ready for OT&E. MCOTEA shall also review all OT&E planning for discussion at the OTRR. OTRR agenda items may be nominated by any OTRR attendee.]

5.6.4 Navy T&E Exceptions

[*fm SNI 5000.2D, 5.6.4: There are two types of T&E exceptions:*]

5.6.4.1 Waivers

[*fm SNI 5000.2D, 5.6.4.1: The term "Waivers" applies to a deviation from the criteria identified for certification in paragraph 5.6.1 of this enclosure. Waivers do not change or delay any testing or evaluation of a system.*]

Waivers are meant to allow a system to enter OT&E even though all the selected criteria in paragraph 5.6.1 – DON Criteria for Certification, Certification of Readiness for Operational Testing, have not been met. Waivers generally do not change or delay any system or testing requirements, nor affect the scope of the OT. Waivers apply only to the data or system maturity identified for entrance into the OT period.

Waivers are not normally requested for EOA or OA periods. Unless otherwise directed by the MDA, waiver requests are appropriate for only OT periods that support FRP or fielding decisions. Before requesting any waiver, the PM should be confident that the program is on track and the system will achieve overall effectiveness, suitability, and survivability during IOT&E.

Data for any waived criteria may be used in COMOPTEVFOR's final analysis to resolve COIs, determine system operational effectiveness, operational suitability, and any recommendation regarding fleet introduction.

5.6.4.2 <u>Deferrals</u>

[***fm SNI 5000.2D, 5.6.4.2: The term "Deferrals" applies to a delay in testing requirements directed by the TEMP. A deferral moves a testing requirement from one test period to a later period. Deferred items cannot be used in the analysis to resolve COIs; however, the OTA may comment on operational considerations in the appropriate sections of the test report. A deferral does not change the requirement to test a system capability, function, or mission, only the timeframe in which it is evaluated.***]

Deferrals are meant to appropriately delay planned testing from one test period to a later test period that can be predicted, funded, scheduled and agreed on by key stakeholders below. Deferrals do not change the quantitative or qualitative value of a requirement, only the timeframe that it will be tested.

5.6.4.2.1 <u>When Deferrals are Appropriate</u>

[***fm SNI 5000.2D, 5.6.4.2.1: Deferrals will not normally be granted for EOAs, OAs, or any OT&E prior to IOT&E. Performance shortfalls should be identified sufficiently early to document system capability maturity in the appropriate CDD, CPD, and TEMP. When unanticipated problems with system maturity or test resources would unduly delay an OT period, deferrals provide for continued testing and efficient use of scheduled resources (e.g., ranges, operational units, and assets).***]

Deferrals for OT&E periods may only be granted after the program and resource sponsors have justified that the system is necessary, useful, and adds capability to the fleet despite deviating from testing of a particular TEMP requirement. (See paragraph 5.6.4.3 below) COMOPTEVFOR will then make a determination on adequacy of the test and a recommendation to conduct or delay testing because of deferral requests. Deferrals

should not be requested for EOA or OA periods. Early assessments of all capabilities help identify risks, unforeseen problems, or provide information useful to system design.

5.6.4.2.2 Limitations to Test

[***fm SNI 5000.2D, 5.6.4.2.2: A deferral may result in limitations to the scope of testing that may preclude COMOPTEVFOR from fully resolving all COIs.***]

5.6.4.2.3 Resolution of COIs

[***fm SNI 5000.2D, 5.6.4.2.3: Deferred items cannot be used in the analysis to resolve COIs; however, the OTA may comment on operational considerations in the appropriate sections of the test report.***]

Because a function, sub-system, or mission capability is not ready for operational testing, a deferral allows relief from the TEMP requirement to test and evaluate data that would knowingly be collected against an immature capability; yet provide an opportunity to evaluate the overall system capabilities that have been identified as adding needed and useful capability to the fleet. The deferral documents the need for future investment to achieve the desired capability for the decision authority, while allowing the OTA to focus reporting on the known capability to date. However, the OTA should provide comments on the operational perspective of employing the system without the deferred capability/item.

5.6.4.3 CNO (N091) Approval of a Deferral Request

[***fm SNI 5000.2D, 5.6.4.3: Deferrals for OT&E periods may only be granted after the program and resource sponsors have justified that the system is necessary and useful, and adds capability to the fleet despite deviating from testing of a particular TEMP requirement. COMOPTEVFOR will then make a determination on adequacy of the test and a recommendation to conduct or delay testing because of deferral requests. The necessary programmatic inputs or changes to account for required additional test periods in which the deferred items are to be tested must be approved by the resource sponsor and official concurrence relayed to CNO (N091). For programs on the OSD T&E Oversight List, the deferral(s) must be coordinated with DOT&E prior to CNO (N091) approval. Approval of deferral requests does not alter the associated requirement, and approved deferrals shall be tested in subsequent operational testing.***]

5.6.5 Navy Waiver and Deferral Requests

[***fm SNI 5000.2D, 5.6.5: Waivers and deferrals shall be requested in the OT&E certification message. If a waiver or deferral request is anticipated, the PM shall coordinate with the***

program sponsor, CNO (N912), and COMOPTEVFOR prior to the OTRR or similar review forum. Deferrals shall be identified as early as possible, normally no later than 30 days prior to OTRR. Use of the T&E WIPT or similar forum is also recommended to ensure full understanding of the impact on operational testing.

When requesting a waiver or deferral, the PM shall outline the limitations the deferral or waiver will place upon the system under test and their potential impacts on fleet use. Further, a statement shall be made in the OT&E certification message noting when approved deferrals will be available for subsequent OT.]

See recommended certification message format found in Annex 5-E of Enclosure (5) in this guidebook for submitting requests.

5.6.6 Marine Corps Waivers

[***fm SNI 5000.2D, 5.6.6: If full compliance with the certification criteria is not achieved, but the deviations are minor, MARCORSYSCOM shall request in the certification correspondence that MCCDC (C441) grant a waiver to allow OT to begin. Justification shall be provided for the waivers. DAs/PMs shall make every attempt to meet all readiness criteria before certification. If the need for a waiver is anticipated, the PM shall identify the waiver to MARCORSYSCOM (Chief Engineer) when establishing the schedule for the OTRR. Waivers shall be fully documented prior to the OTRR.***]

5.7 Operational Test and Evaluation (OT&E)

5.7.1 Independent OT&E

[***fm SNI 5000.2D, 5.7.1: Reference (b) requires an independent organization, separate from the DA and from the user commands, be responsible for all OT&E. OT&E shall be conducted by the OTA or an agent designated by the OTA for ACAT I, IA, II, III, and IVT programs. COMOPTEVFOR and the Director, MCOTEA, are responsible for planning and conducting OT&E, reporting results, providing evaluations of each tested system's operational effectiveness and suitability, and identifying and reporting system deficiencies. Additionally, COMOPTEVFOR is responsible for providing inputs to tactics, as appropriate, and making recommendations regarding fleet introduction. OT shall determine whether thresholds in the CDD/CPD have been satisfied. See reference (b), enclosure 5, for implementation requirements for all DON ACAT programs requiring OT&E.***]

5.7.1.1 Navy Start of OT&E

[*fm SNI 5000.2D, 5.7.1.1: COMOPTEVFOR may commence operational testing upon receipt of a certification message unless waivers or deferrals are requested. When waivers or deferrals are requested, COMOPTEVFOR may start testing upon receipt of waiver or deferral approval from CNO (N091). COMOPTEVFOR shall issue a start test message when OT begins.*]

5.7.1.2 Navy De-certification and Re-certification for OT&E

[*fm SNI 5000.2D, 5.7.1.2: When evaluation of issued deficiency/anomaly reports or other information indicates the system will not successfully complete OT&E, de-certification may be originated by the SYSCOM Commander/PEO/DRPM, after coordination with the program sponsor and PM, to withdraw the system certification and stop the operational test. Withdrawal of certification shall be accomplished by message to CNO (N091) and COMOPTEVFOR stating, if known, when the system will be evaluated for subsequent certification and restart of testing. When a system undergoing OT&E has been de-certified for OT, the SYSCOM Commander/PEO/DRPM must re-certify readiness for OT&E prior to restart of OT per paragraph 5.6.2.*]

5.7.2 OT&E Plans

[*fm SNI 5000.2D, 5.7.2: See reference (b), enclosure 5, for implementation requirements for DON ACAT programs requiring OT&E. ACAT I, II, and programs on the OSD Oversight list require DOT&E approval.*]

5.7.2.1 OT&E Phases and Procedures

OT&E can consist of operational assessments (OAs), verification of corrected deficiencies (VCD), software qualification test (SQT), the independent phase of OT during "combined DT/OT," IOT&E, and FOT&E. All forms of OT&E require compliance with reference (b), covered by SECNAVINST 5000.2D, enclosure (5), paragraph 5.6. With evolutionary acquisition, a program may have multiple IOT&Es as new increments of requirements are added to the development. For each program, or program increment under development, COIs should be developed by the OTA and published in part IV of the TEMP. The COIs are linked to CNO or CMC capability needs established in the CDD/CPD and are evaluated while conducting scenarios that are representative of the system’s operational environment and workload of typical users. The phases listed below should be tailored through further sub-division, as required. Annex 5-D depicts a notional schedule of OT phases within the phases of the acquisition model.

5.7.2.1.1 Operational Assessments (OAs)

Operational Assessments are conducted by an independent OTA. The focus of an OA is to assess trends noted in development efforts, programmatic voids, risk areas, adequacy of requirements, and the ability of the program to meet performance goals in operational effectiveness and suitability. OAs can be made at any time using technology demonstrators, prototypes, mockups, or simulations, but do not substitute for the IOT&E necessary to support FRP decisions. An OA does not have to use production representative articles. An MDAP or OSD designated T&E oversight program requires an OA to support a LRIP decision, and can support other program reviews. All OAs are included in Part IV and V of the TEMP. For programs on the OSD T&E oversight list, the OA test plans require formal approval by DOT&E. OAs do not support VCDs, FRP DRs, fleet release or introduction recommendations.

5.7.2.1.2 OT-A (EOAs)

Early operational assessments (EOAs) are conducted during the Concept Refinement and Technology Development phases to support Milestone B. Tests should employ advanced development models (ADMs), prototypes, brass-boards, or surrogate systems, but may be limited to virtual models. The primary objectives of an EOA are to provide early identification of risk areas and projections for enhancing features of a system. An OT-A (EOA) should be considered for ACAT I and II programs, other programs receiving DOT&E oversight, and other ACAT programs, as appropriate.

5.7.2.1.3 OT-B (OA)

OT-B is the OA conducted during the System Development and Demonstration phase. For most ACAT I and OSD DOT&E oversight programs, at least one OA is a prerequisite for LRIP. The MDA should determine if OT&E is required prior to LRIP for non-OSD T&E oversight programs. If there are two or more phases of OT-B, the final phase will support Milestone C (LRIP approval).

5.7.2.1.3.1 DT Assist

Whenever appropriate, in order to reduce program costs, improve program schedule and provide early visibility of performance risk, COMOPTEVFOR or Director, MCOTEA may be asked by the PM to assist DT&E. This is a DT phase, under the control of the DA and the requirements of DT&E are in effect. DT assist is not a formal phase of OT&E, but rather a period of DT in which OT personnel are actively involved, providing operational perspective, and gaining valuable hands-on familiarity with the system. Data and findings from DT assist may be used to supplement formal OT data. DT assist does not resolve COIs, does not reach conclusions regarding operational effectiveness or suitability, and does not make a recommendation regarding fleet

release. An OT&E test plan or OT&E final report is not generated. A letter of observation (LOO) is provided to the DA upon request.

COMOPTEVFOR and Director, MCOTEA should participate in DT&E planning, monitor DT&E, assess relevant OT&E issues, and provide feedback to the DA for DT assist periods. This involvement in DT&E planning allows maximizing the use of DT data by the OTA by fixing the conditions under which DT data meets the operationally realistic conditions to allow its use by the OTA for analysis.

A memorandum of agreement (MOA) may be developed between COMOPTEVFOR or Director, MCOTEA and the DA for all DT assisted DT&E. This MOA should address sharing of data, contractor involvement, and level of feedback from the OTA to the DA.

5.7.2.1.4 <u>OT-C (IOT&E)/(Navy OPEVAL)</u>

IOT&E is OT&E conducted to support a FRP decision by the MDA or a recommendation by the OTA for a fleet release or fleet introduction. It consists of the OT&E in the Production and Deployment phase before the FRP decision.

Equipment/software introduced into the tested system for IOT&E should be production representative. See this guidebook, enclosure (5), paragraph 5.7.2.2, for software IOT&E requirements. The level of system development should be documented in the TEMP parts III and IV. IOT&E should commence upon the DA's certification of readiness for OT or upon receipt of approval by CNO (N091) (see SECNAVINST 5000.2D, enclosure (5), paragraphs 5.6.4.4 and 5.6.6) when required due to waiver or deferral. The time allotted between completion of IOT&E and the Full-Rate Production Decision Review should allow adequate time (normally 90 days for ACAT I and II programs, and 60 days for ACAT III and IVT programs) for preparing the evaluation report by COMOPTEVFOR and additional days (normally 45) for review by OSD DOT&E plus any additional time required by the DA to plan for discrepancy correction. If production or fleet introduction is not approved at Full-Rate Production Decision Review, subsequent T&E should be identified as further phases of DT-C and OT-C. If the system is approved for acquisition of additional LRIP quantities because significant deficiencies remain, CNO may schedule an additional phase of IOT&E.

5.7.2.1.5 <u>Combined DT/OT</u>

Combined DT and OT is a period of test in which assets and data are shared by the DA and COMOPTEVFOR or Director, MCOTEA to reduce program costs, improve program schedule, and provide visibility into performance risk early in the testing cycle. If the DA and OTA desire to combine DT and OT such that OT data is obtained, reference (b) OT requirements and OT requirements of SECNAVINST 5000.2D, paragraph 5.7.1, need to be met. If during

combined DT/OT a dedicated period of OT is necessary, this dedicated period will be exclusively OT, generally near the end of the combined testing, and executed by COMOPTEVFOR or Director, MCOTEA. A dedicated OT period permits the OTA to assess system performance in as operationally representative environment as possible. COMOPTEVFOR or Director, MCOTEA should participate in DT&E planning, monitor DT&E, assess relevant OT&E issues, and provide feedback to the DA. Specific conditions and responsibilities that cannot be adequately covered in the TEMP, including the sharing of test data, should be outlined via a MOA between the DA and COMOPTEVFOR or Director, MCOTEA. While TECHEVAL and IOT&E cannot be combined, operationally relevant TECHEVAL data may be used to supplement data collected during IOT&E.

5.7.2.1.6 Follow-on Operational Test and Evaluation (FOT&E)

FOT&E is all OT&E conducted after the final phase of IOT&E.

5.7.2.1.6.1 OT-D

OT-D is OT conducted after the FRP decision. OT-D is conducted, if appropriate, to evaluate correction of deficiencies in production systems, to complete deferred or incomplete IOT&E, and to continue tactics development.

5.7.2.1.6.2 OT-E

OT-E should be scheduled and conducted to evaluate operational effectiveness and suitability for every program in which production models have not undergone previous OT&E.

5.7.2.1.6.3 Verification of Corrected Deficiencies (VCD) for Navy Programs

While specific OT report tracking and response mechanisms are not required, programs should review OT reports and formally respond with plans for addressing or deferring the correction of deficiencies. The purpose of VCD is to confirm correction of deficiencies identified during IOT&E or FOT&E. This evaluation should apply to only those deficiencies that have been corrected. VCD can occur through COMOPTEVFOR review and endorsement of corrective actions or, in some cases, through an end-to-end test of the complete system, depending on the complexity of the system and the extent of the deficiencies. Where retest of deficiencies is required, a VCD can occur as part of formal FOT&E or as a specific test limited to the verification effort. The DA should submit VCD requests to COMOPTEVFOR with an information copy to

CNO (N091). The TEMP need not be updated/revised prior to a VCD. Rather, the VCD and its results should be incorporated in the next scheduled TEMP update/revision. The VCD request to COMOPTEVFOR from the DA should identify the deficiency(ies) corrected.

An OTRR is not required prior to commencing a VCD.

5.7.2.1.7 <u>OT Resource Requirements</u>

To avoid cost growth, the OTA should advise the DA of OT&E resource requirements early in test planning and prior to TEMP approval. When resource requirements cannot be specified prior to TEMP approval, a time and/or methodology should be provided to complete resource requirements for test. The OTA should maintain continuous close liaison with the PM/DA over the life of the program. For Navy programs, CNO (N091) resolves issues when there is a disagreement between the DA and the OTA.

5.7.2.2 <u>OT of Computer Software</u>

Computer software presents unique OT challenges. Successful programs are following the methodology and philosophy herein to develop their software testing programs.

Within its lifecycle, software development and deployment can be broken into two categories:

1. New Developments that represent or will represent the first fielded version of the software, which will be called herein the baseline or core increment, and

2. Revisions to the baseline that are or will be fielded, which will be called herein increments one, two, etc. in sequential order of development. Any software code modification, no matter how minor, will be considered a revision to allow management of OT configurations as needed.

Software works within a hardware/software construct, which includes the computer hardware that executes the software, and other hardware and software with which the software interacts or affects. Herein this construct is called a configuration.

Any changes to the hardware or software in the construct changes the configuration and is a key factor in deciding the amount of testing required for each software revision. Strong configuration management is an absolute requirement for keeping program risks and software testing costs to a minimum.

Typically, DT of software involves verification that the specified functionality works as contracted and that the software does not cause a fatal computer fault. However, even the best DT is unable to fully test the code, often follows non-operational test scenarios and may not subject the system to operational

environmental stresses. For this reason as well as for regulatory and statutory reasons, OT is required.

The subsections of this guidebook below address the best way to conduct operational software testing for most acquisition systems. It is based upon proven successful software testing practices already in use within DoD. Annexes 5-E, 5-F, and 5-G to this enclosure provide additional guidance on determining elements of risk, the appropriate level of testing, and responsibilities.

5.7.2.2.1 Baseline or Core Increment Testing

OT planners should examine and consider the DT conducted in their planning for OT&E. They must also know the differences between the DT configuration and the operational configuration. Assuming that the DT is assessed by the OTA to have met its goals and the configuration differences are not major, OT planners should proceed to plan OT&E, which permits assessment of the software's effectiveness, suitability, and survivability in fully realistic operational scenarios, with real users, in operational environments. Where DT is assessed by the OTA to meet OT data needs, actual OT may be reduced as appropriate. It is emphasized that the decision to use or not use DT data is that of the OTA, not the DA.

5.7.2.2.1.1 Mission Criticality/Software Risk Based Operational Testing

Just as DT&E cannot exhaustively test software for all conditions, neither can OT&E. Given this reality, OT&E must follow a methodology that focuses first and foremost on the primary concerns of the operational user with attention given to secondary concerns as time and resources permit.

The most accepted software OT&E methodology within DoD is to prioritize software testing in order of highest mission criticality and highest software risk.

Software risk (SR) is characterized by what is known about its functionality and reliability. If software is known by previous operational experience and testing to properly function and be reliable then the risk is low.

Mission criticality (MC) is characterized by the impact of software failure on operational mission success. If software failure could cause mission failure, the MC is high.

Combining these two concepts, software that has high MC and high SR should be tested as thoroughly as possible. On the other hand, the need to thoroughly test software with a low MC

and low SR is less urgent. Additional guidance on how to apply these concepts in a manner acceptable to test approval authorities is found in the Annexes 5-E and 5-F to enclosure (5).

5.7.2.2.2 Revision or post Core Increment Testing

Testing software revisions to a baseline follows the same methodology as for baseline or previous increment testing. The only expected difference is in the level of risk assigned to the software. Because there should be some increased knowledge of and therefore increased level of confidence in the software functionality and reliability, the level of OT&E may be tailored further than in baseline or previous increment OT&E. However this could be offset by configuration changes. OT planners must carefully examine how a software increment differs from its predecessor as well as any configuration changes before reducing the scope of OT&E. Again the effect on mission success should the software increment fail must play a role in deciding the scope of OT&E.

5.7.2.2.3 Use of Non-Operational Facilities

Use of Non-Operational Facilities (e.g., LBTS) to conduct part or all of OT is encouraged. To the extent that such a facility fully replicates the operational environment in all details, data derived therein may be used by the OTA for OT&E purposes. Where there are differences to the complete operational environment, OT must be conducted in the intended operational environment when physically possible to assess those differences. By operational environment replication, it is meant to include such factors as size, shape, air conditioning, power fluctuations, and any other physical factor that causes the facility not to fully replicate the actual operational environment. Further, human factor differences must be evaluated as well. For instance, the test operators should be actual military operators of the same training, ranks, rates, backgrounds, and abilities as found in the operational environment. Well-documented, strong configuration management of such facilities is necessary to allow their use in OT&E.

5.7.2.2.4 Use of Modeling, Simulation, and Signal Stimulation in Software Testing

Modeling and Simulation (M&S) may be used for operational test planning and justification by the OTA for limiting the scope of OT&E but cannot be used in lieu of OT&E. Use of M&S to augment OT&E results should be limited to those cases where actual OT&E cannot be conducted by law or by limitations in testing technology or resources.

Use of artificial signals or data to simulate real world operational inputs in support of software OT&E is permitted when, in the opinion of the OTA, real world data or signals cannot be obtained in a manner to support OT&E objectives, resources, or

time limits.

Use of M&S or artificial signals or data in support of OT&E planning or results should be documented in the OT&E report. All M&S used to support OT&E should meet V&V standards of reference (c) and be accredited by the OTA for its specific use.

5.7.2.2.5 Use of Non-Operational Test Agency (OTA) Testers to Conduct OT&E

The OTA is encouraged to consult and use software experts and non-resident software testing resources as required to plan for or to satisfy OT&E objectives. This includes use of software testing tools. However, reliance on outside expertise and tools to interpret OT results or to conduct OT must be limited to those cases where the OTA lacks the resources to do otherwise and must be documented in the OT&E report. Reliance on tools, models, and expert opinions is more in the domain of DT&E. OT&E must remained focused on how a system actually works in the real world, not how it is predicted to work by tools, models, or experts.

5.7.2.2.6 Role of the Developing Activity (DA) and the OTA in OT&E of Software

The OTA is responsible to conduct OT&E of software in as realistically a manner as is possible. The OTA is encouraged to tailor OT&E and especially OT&E in the actual operational environment as suggested in this guidebook and by other DoD regulations, instructions, and guidance. However, for the OTA to tailor OT&E of software, he must have proof that such tailoring is defensible.

The DA is responsible for providing all the information required by the OTA to make a determination of how and to what extent he may tailor OT&E.

The best way to optimize software testing is for the DA and OTA to meet early and often to establish and refine software-testing criteria and to establish and refine data requirements necessary to permit tailoring software tests.

5.7.2.2.7 Designation of Software Testing and Software Qualification Testing (SQT)

When a software revision or increment is to be released as part of an acquisition milestone decision, the OT is considered to be an OA or IOT&E. When a software revision or increment is to be released not in conjunction with a milestone decision, it may be designated a Software Qualification Test (SQT).

5.7.2.2.8 Software Operational Testing and Interoperability, Security, or Information Assurance Certification

Various organizations have been established to "certify" or "accredit" software for interoperability, security, or IA. Certification or accreditation of software by an outside agency or authority does not absolve the OTA from operationally testing and assessing software for interoperability, security, or IA. As with DT data, the OTA is encouraged to consider and use certification or accreditation data to assist in their assessments and to tailor OT&E accordingly, but the use of such data must be defensible as being operationally as realistic as possible. Whether to use certification or accreditation data in support of or in lieu of some OT&E is the decision of the OTA.

5.7.2.2.9 Changes to Software Operational Requirements

Operational testers assess software for effectiveness, suitability, and survivability in conformity with the approved operational requirement for the software documented in the ICD, the CDD, and the CPD or their predecessors, the Mission Needs Statement (MNS) and the Operational Requirements Document (ORD). The TEMP is the formal agreement regarding what to test, when, and with what resources.

The situation sometimes arises, and is expected to occur more often with Evolutionary Acquisition, where a software revision adds capability not addressed in the formal capabilities (requirements) documents or deletes or defers formal capabilities needs. When such a change adversely affects the formal capability need in a significant way then the formal capabilities documents and TEMP should be modified and approved accordingly. Note that any changes to software operational capabilities require an assessment for human systems integration (HSI) and doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) implications. The implications for each increment should be identified, planned, documented, and accepted by CNO (N1) and CNO (N12) prior to formal approval of revisions to operational capabilities documents. When such a change does not adversely affect the formal requirement in a significant way, then the operational testers may accept a Statement of Functionality (SOF) approved by the appropriate resource sponsor, as the basis for modifying the OT plan objectives. The OT report should note the requirement and test modification and its approval by the resource sponsor.

5.7.2.2.9.1 Statement of Functionality (SOF)

The SOF is normally prepared by the PM for use by the OTA and routed via the PM’s chain of command through the Resource

Sponsor (to include coordination with CNO (N1) and CNO (N00T)) to CNO (N091) for approval for Navy programs. The SOF should include as a minimum:

1. The additions, deletions, and modifications to the software capability,

2. The reason for making the changes and not following the formal requirements plan and delivery schedule,

3. How the additions, deletions, or modifications affect the overall satisfaction of mission need in the formally stated requirement,

4. Why a formal change to the capabilities documents or TEMP is not considered necessary,

5. How the additions, deletions, or modifications affect KPPs, CTPs, COIs, or Measure of Effectiveness (MOE) in existing capabilities documents and TEMPs/Test Plans, and why this is acceptable, and,

6. Additional testing requirements or concerns raised by the additions, deletions, or modifications that should be factored in the test planning or execution.

5.7.2.2.10 System of Systems Testing

The DoD is investing tremendous effort into the development and fielding of software intensive systems that work in a single net centric continuum (e.g., FORCEnet and the Global Information Grid (GIG)). The issue arises as to how to test a system that must connect and become a part of a larger SoS. DoD and DON guidance is evolving but leaves no doubt that such systems must be operationally effective, suitable, and survivable in the SoS.

The threat of the use of our net centric systems against us by potential enemies makes the effectiveness of both IA and Information Security (IS) an important COI for test planners to address. Not only must each new system attached to the net be operationally effective and suitable in its own right, it must also be proven to not create an IA or IS threat to the net by enemy action. That enemy action is not only an external one but also an internal one. IA and IS threats are emerging that show the need to have system protections in depth against agents both outside and inside system security boundaries and protocols.

OT planners should focus their testing of systems that connect to SoS as follows.

1. Assess the system's operational effectiveness, suitability, and survivability per the overall guidance of this enclosure on software testing.

2. Assess the system's interoperability with the SoS in mission critical operational scenarios. Limit assessment of potentially adverse impacts on the SoS by the system to this interoperability testing.

3. Assess the IS and IA vulnerability posed by the system on the SoS in operationally realistic scenarios. Assume that the system or its portal to the SoS is the source of the attack. Look at attacks coming through the portal to the system and from the system through the portal to the SoS. Do not try to assess in what manner the SoS could be impaired by an attack but simply report the vulnerability. Do not assess IS or IA of the SoS.

Cryptographic systems used to protect systems or the SoS should be assumed to be secure but their potential capture or use by inside hostile agents as a means to conduct information warfare attacks on either the system or through the system to the SoS should be operationally evaluated. If in the course of testing, cryptographic security issues become evident, they should be immediately addressed to NSA through proper DON and DoD channels and to CNO (N091) for adjudication.

SoS testing guidance is undergoing continual evaluation and development. Data, results, conclusions, opinions, and recommendations concerning this testing guidance and SoS testing in general should be sent to OPNAV N912 for consideration in the update to both T&E policy and recommendations in this guidebook.

5.7.2.2.11 <u>Resolution of Disputes involving Operational Testing of Software</u>

Disagreements between parties involved in software test planning and execution (e.g. DA, Resource Sponsor, OTA, etc.) should be resolved primarily through the T&E WIPT. Navy programs may seek interpretation of test policy from OPNAV N091/N912.

Should the T&E WIPT not resolve an issue, the parties involved should request adjudication by the TECG for Navy programs or the IPPD process for Marine Corps programs.

5.7.3 <u>Operational Test (OT) for Configuration Changes</u>

[***fm SNI 5000.2D, 5.7.3: The DA shall ensure the T&E planning includes OT&E for significant configuration changes or modifications to the system. These OT&E events are necessary for the OTA to substantiate a fleet release/introduction recommendation to the CNO/CMC for all systems.***]

See paragraphs 5.7.2.2.2, 5.7.2.2.9, and 5.7.2.2.9.1 in this guidebook.

5.7.4 <u>OT for Information Assurance and System Security Certification and Accreditation</u>

[*fm **SNI 5000.2D, 5.7.4:** All weapon, C4ISR, and information programs shall be tested and evaluated for appropriate application of information assurance (IA) (reference (b)). Systems shall incorporate IA controls identified in reference (e), based upon the objective of MAC and Confidentiality Level. The OTA shall operationally test and evaluate IA controls (i.e. people, technology, and operations) to the level of robustness specified by the objective of the MAC and Confidentiality Level against DIA/ONI validated IA threats per reference (d). IA controls should be evaluated for adequacy and tested for compliance. Evaluation of the SoS or FoS in which the subject system operates should be minimized to the scope necessary to resolve COIs for the subject system.*]

See paragraphs 5.7.2.2.8 and 5.7.2.2.10 in this guidebook.

5.7.5 <u>Quick Reaction Assessment (QRA)</u>

[*fm **SNI 5000.2D, 5.7.5:** When an urgent operational need is identified for a system in development or when a system has been granted RDC status (as defined in enclosure (2), paragraph 2.8) by ASN(RDA), it may be necessary to modify the established OT process to rapidly deliver that capability to the fleet. In such cases, the program sponsor may obtain an OTA assessment of operational effectiveness, suitability, and considerations for deploying the system. Navy program sponsors may request a QRA from CNO (N091). USMC program sponsors may request a QRA from Director, MCOTEA. When approved, COMOPTEVFOR or Director, MCOTEA should conduct the assessment and issue a report as soon as possible. The following information should be included in the QRA request:*

1. The purpose of the assessment and, specifically, what system attributes the program sponsor wants assessed.

2. The length of time available for the assessment.

3. The resources available for the assessment.

4. Which forces will deploy with the system prior to IOC.

QRAs do not obviate or replace scheduled OT in an approved TEMP for programs of record. Systems in RDC status that have completed QRA will normally undergo formal OT when they transition to program status.]

5.7.6 OT&E Information Promulgation

[***fm SNI 5000.2D, 5.7.6: See reference (b), enclosure 5, and this enclosure, paragraph 5.11, T&E Reports, for information promulgation requirements for all DON ACAT programs requiring OT&E.***]

5.7.6.1 Milestone Decision Authority (MDA) Briefing

[***fm SNI 5000.2D, 5.7.6.1: See reference (b), enclosure 5, for implementation requirements for DON ACAT I and IA programs and programs on the OSD T&E Oversight List. The OTA will brief the results of program OTs at MDA decision meetings.***]

5.7.6.2 OT Data Release

The OTA should release valid data and factual information in as near real-time as possible to the DA. Data may be preliminary and should be identified as such. Evaluative information should not be released until the OTA has completed its evaluation and issued a final report. Anomaly reports and deficiency reports will be issued as explained in this guidebook, enclosure (5), paragraph 5.11.1.2. The logistics of releasing data should not interfere with test events, analysis, or report preparation.

5.7.7 Use of Contractors in Support of OT&E

[***fm SNI 5000.2D, 5.7.7: See reference (b), enclosure 5, for implementation requirements for DON ACAT programs requiring OT&E.***]

5.7.8 Visitors

[***fm SNI 5000.2D, 5.7.8: During operational testing, observers and other visitors are authorized at the discretion of COMOPTEVFOR, or Director, MCOTEA, as appropriate.***]

Note that per reference (t), visit clearances through the Foreign Visits Systems are required for foreign national observers or visitors to government facilities.

5.7.9 Special T&E Considerations

5.7.9.1 T&E of Modifications

The recommendations of COMOPTEVFOR, the DA, the CNO resource and program sponsor(s), and INSURV and ASN(RD&A) CHSENG (both where applicable) should be considered in a T&E WIPT forum, as described in paragraph 5.4.3 of this guidebook, in determining

the scope of testing. CNO (N091) should adjudicate unresolved issues concerning testing of modified systems and software. See also paragraph 5.7.3 above.

5.7.9.2 T&E of Non-Developmental Items/Commercial-Off-The-Shelf (NDI/COTS)

Prior to an NDI/COTS acquisition decision, the DA, with the concurrence of COMOPTEVFOR/MCOTEA, should assess the adequacy of any previously conducted DT&E, OT&E, contractor, or other source data and provide recommendations to CNO (N091)/CMC (DC,CD&I) on the need for additional T&E requirements. When the procurement of a system developed or tested by a non-DON DA is being planned, a memorandum of understanding (MOU) between the activities involved should address the acceptance of prior T&E results. If additional T&E is required, the DA should initiate a TEIN request.

5.7.9.3 Extension of Application

An extension of application eliminates the requirement for IOT&E/OPEVAL by COMOPTEVFOR/Director, MCOTEA for the common system, subsystem, or equipment that have previously undergone IOT&E in other platforms, systems, etc. Concurrence of the suitability of extension of application should be obtained via the OTA. Extension of application does not eliminate the need to obtain fleet introduction approval from the program sponsor. A period of FOT&E should be considered to verify that integration of the system, subsystem, or equipment into the host platform has not degraded performance. Following FOT&E, the program sponsor should determine if full fleet introduction or installation is appropriate.

5.8 Annual Office of the Secretary of Defense (OSD) T&E Oversight List

[*fm **SNI 5000.2D, 5.8: DOT&E annual oversight list identifies those DON programs subject to DOT&E oversight. ACAT I, II, and programs requiring LFT&E are generally included in oversight. Other programs that generate Congressional, public, or special interests are routinely included in the listing. DON T&E information related to programs on the OSD Oversight list will be coordinated through CNO (N091) for Navy programs. PMs for USMC programs subject to OSD T&E oversight will coordinate DT information, and Director, MCOTEA, will coordinate OT information.***]

5.9 Live Fire Test and Evaluation (LFT&E)*

[*fm **SNI 5000.2D, 5.9: The DA is responsible for LFT&E strategy development, associated TEMP input, monitoring, and supporting the conduct of LFT&E. Per reference (b), DOT&E shall approve the LFT&E strategy for programs covered by statute prior***

to the decision to enter into SDD (normally Milestone B). For USMC programs not required by statute to conduct LFT&E, but where LFT&E is appropriate, the Director, MCOTEA, shall concur with the LFT&E strategy as approved by the MDA in the TES or TEMP.

Per 10 U.S.C. Section 2366, realistic survivability and lethality testing shall be completed, the report submitted, and results considered, prior to making a beyond LRIP decision.

Survivability and lethality tests required by statute must be completed early enough in SDD phase to allow correction of any design deficiency before proceeding beyond LRIP.

LFT&E events deemed necessary prior to Milestone B may be conducted under a stand-alone plan (in lieu of an approved TEMP). The intention of this policy is to facilitate agreement between developers and oversight agencies. This stand-alone plan for pre-Milestone B LFT&E events will follow the same approval process as prescribed for a TEMP. The stand-alone plan should be limited in scope and address only objectives of pre-Milestone B LFT&E events. Subsequently, the stand-alone plan should be integrated into the TEMP.

Each program increment or modification requires a review for LFT&E requirements. If such requirements are found to exist, they must be addressed through the TEMP process.

See reference (b), enclosure 5, for implementation requirements for a program that is a covered major system, a major munitions program, a missile program, or a product improvement (modification) thereto. A covered major system means a vehicle, weapon platform, or conventional weapon system that provides some degree of protection to users in combat and is a major system per 10 U.S.C. Section 2302(5). A major munitions program means a program that is planning to acquire more than a million rounds or is a conventional munitions program that is a major system.

****Not applicable to ACAT IA programs.***]

5.9.1 <u>LFT&E of Ships</u>

For ships, the qualification of the survivability baseline is conducted during construction and shakedown. During construction, tests and inspections confirm the achievement of compliance with the requirements of the shipbuilding specification in the areas of shock hardening, air blast hardening, fire containment, damage control features, structural hardening, and chemical, biological, and radiological (CBR) protection. During the 1-year shakedown period following delivery of the lead ship of a class, or early follow ship as determined per reference (u), a full-ship shock trial should be conducted to identify any unknown weakness in the ability of the

ship to withstand specified levels of shock from underwater explosions.

5.10 Foreign Comparative Testing (FCT)

5.10.1 Programs Defined by Statute

[***fm SNI 5000.2D, 5.10.1: 10 U.S.C. Sections 2350a(g) and 2359b establish two programs: the Foreign Comparative Testing (FCT) Program and the Defense Acquisition Challenge Program (DACP). The FCT program tests allied or friendly nations' defense equipment, munitions, and technologies to see if they can satisfy DoD needs. DACP allows non-DoD entities to propose technologies, products, or processes to existing DoD acquisition programs. At the OSD level, both FCT and DACP are managed by the Comparative Testing Office (CTO) (http://www.acq.osd.mil/cto/organization.htm) under USD (AT&L/DDRE/DUSD(AS&C)).***]

The FCT program provides for the test and evaluation of foreign non-developmental equipment that demonstrates potential to satisfy an operational requirement. Within the DON, Navy IPO proposes and manages FCT projects. Each year Navy IPO issues a call for proposals to the System Commands (MARCOR, NAVAIR, NAVSEA, SPAWAR). Proposals are prioritized by either CNO or HQ USMC prior to Navy IPO submission to DUSD(AS&C). Navy IPO oversees the project management of all DON FCT projects via the System Commands. Proximate project management is delegated to the Systems Commands, who report to Navy IPO on technical, schedule, and financial status.

5.10.2 Navy Management of Comparative Testing

[***fm SNI 5000.2D, 5.10.2:***

1. For FCT: Navy International Programs Office (Navy IPO) (https://www.nipo.navy.mil/)

2. For DACP: Office of Naval Research (ONR), Code 36, DACP Office

(Note: As of the date of this publication, Navy management of DACP is under review and may change.)]

Congress recently initiated the DACP, which is intended to encourage the test and evaluation of innovative technology for use in meeting validated operational requirements. OUSD(AT&L)'s Comparative Testing Office has overall responsibility for this program. DON proponents should consult DASN(RDT&E) for Navy-specific guidance in participating in the DACP.

5.10.3 Developing Activity (DA) Comparative Testing Responsibilities

[*fm SNI 5000.2D, 5.10.3: DAs shall follow comparative testing guidance provided by OSD (CTO) and the Navy points of contact cited above. Where comparative testing is a major portion of an acquisition program, it should be included in the TEMP. Comparative testing derived components of an acquisition program shall be treated like contractor Non-Developmental Items (NDI). Acquisition programs, that include comparative testing derived items, are not exempt from DT, OT, or LFT&E provisions of this instruction. Reference (b), enclosure 5, provides DoD direction on comparative test programs.*]

5.11 Test and Evaluation Reporting

[*fm SNI 5000.2D, 5.11: This paragraph describes mandatory T&E reporting requirements for DON ACAT programs as indicated in subsequent paragraphs. Per reference (b), enclosure (5), section 5.4.8, DOT&E and the Deputy Director for DT&E/Office of Defense Systems (DS) in the Office of the USD (AT&L) shall have full and timely access to all available developmental, operational, and live-fire T&E data and reports. The Defense Technical Information Center (DTIC) provides distribution guidance.*]

5.11.1 DoD Component (DON) Reporting of Test Results

[*fm SNI 5000.2D, 5.11.1: See reference (b), enclosure 5, for implementation requirements for DON ACAT I, selected ACAT IAM, and other ACAT programs designated for DOT&E oversight.*]

5.11.1.1 DT&E Reports

[*fm SNI 5000.2D, 5.11.1.1: A report of results for all DT&E conducted in DON shall be provided to the appropriate decision authority and to the OTA as needed. For programs on the OSD T&E oversight list subject to DOT&E oversight, the DA shall provide copies of formal DT&E reports to the Deputy Director, DT&E in the Office of Defense Systems (ODS) in the Office of the Under Secretary of Defense (Acquisition, Technology and Logistics)(OUSD (AT&L)) and COMOPTEVFOR/Director, MCOTEA at a pre-agreed timeframe prior to program decision point reviews. Copies of DT&E reports for ACAT I programs shall be provided to the Defense Technical Information Center (DTIC) with the Report Documentation Page (SF 298). Copies of Navy internal DT&E event reports shall be forwarded to CNO (N091); the Deputy Director, DT&E; and ASN(RD&A) CHSENG. Unless otherwise coordinated, DT&E reports shall be provided to the OTA at least 30 days prior to start of OT. See reference (v) for distribution statements required for technical publications and reference (w) for principles and operational parameters on DoD Scientific and Technical Information programs.*]

5.11.1.2 Navy OT&E Reports

[*fm SNI 5000.2D, 5.11.1.2: COMOPTEVFOR shall issue OT reports for ACAT I and IA programs within 90 days following completion of testing. All other operational test reports are due within 60 days of test completion. Programs subject to OSD T&E oversight shall provide copies of formal OT&E reports to DOT&E per pre-agreed timeframe prior to program decision reviews. When scheduling a FRP decision review DR, schedulers shall consult DOT&E as to time required to prepare and submit the beyond LRIP report. Copies of OT&E reports for all ACAT I programs, except those that contain vulnerabilities and limitations data for key war-fighting systems, shall be provided to the DTIC with the Report Documentation Page (SF 298). For OSD oversight program T&E events, as defined in the TEMP, copies of Navy OT&E reports shall be forwarded via CNO (N091) to DOT&E and ASN (RD&A) CHSENG. See reference (v) for distribution statements required for technical publications and reference (w) for principles and operational parameters on DoD Scientific and Technical Information programs .*]

5.11.1.2.1 Anomaly Reports

An anomaly report is originated by COMOPTEVFOR when minor failures or anomalies are discovered during operational testing that impact testing, but are not so severe that testing should be stopped. COMOPTEVFOR should report applicable data relating only to this anomaly. The anomaly report is addressed to CNO (N091), the DA, and the program sponsor or information technology (IT) functional area point of contact (POC) for IT programs. COMOPTEVFOR decides when and if to close a specific phase of OT&E for which an anomaly report was issued.

5.11.1.2.2 Deficiency Reports

A deficiency report is originated by COMOPTEVFOR when it becomes apparent that the system under OT&E will not achieve program objectives for operational effectiveness and suitability, is unsafe to operate, is wasting services, or test methods are not as effective as planned. COMOPTEVFOR should stop the test and transmit a deficiency report to CNO (N091), the DA, and the applicable program sponsor, or the IT functional area POC. All deficiency test data should be provided to the DA for corrective action. The information should include the configuration of the system at the time the test was suspended, what specific test section was being conducted, observed limitations that generated the deficiency status, and any observations that could lead to identification of causes and subsequent corrective action. When corrected, the program is recertified for OT&E per SECNAVINST 5000.2D, enclosure (5), paragraph 5.6.2.2. A recertification

message is required, prior to restart of testing, addressing the topics listed in SECNAVINST 5000.2D, enclosure (5), paragraph 5.6.1.

5.11.1.3 Marine Corps Operational Test Reports (TRs)

[*fm SNI 5000.2D, 5.11.1.3: After OT, the FMF shall write the Test Director test report. The TR shall address the collection, organization, and processing of information derived from the OT and is a key source of information from which the independent evaluation report (IER) is written. The report also documents the overall potential of the system to meet operational effectiveness and suitability thresholds. The TR shall be forwarded via the appropriate Marine Force, to arrive at MCOTEA no more than 30 days after the end of the test. The PM does not have a role in developing or reviewing the TR. TRs that will be used to support acquisition activities such as "Down Select" shall be marked "For Official Use Only" (FOUO) by the Director, MCOTEA, and handled appropriately.*

Once approved, MCOTEA shall distribute it to the MDA, PM, FMF, ASN (RD&A) CHSENG, and others concerned including DOT&E for ACAT I, selected ACAT IAM, and other DOT&E oversight programs. Release of the observed test results prior to completion of analysis is as deemed appropriate by the Director, MCOTEA.

The results of EOAs and OAs shall be reported directly to the PM. The time and format for these assessment reports shall be determined by MCOTEA and the PM.]

5.11.1.4 OT&E Reporting Against the Threat of Record

In cases where the threat at the time of testing deviates from the threat delineated in the requirements document, the OTA in coordination with the DA and sponsor should plan testing and evaluation that segregates report results. This enables the MDA and the CNO to have a clear articulation of both the system performance against what was programmed for and what can be expected for Fleet introduction. The value added by reporting in this manner should be determined to exceed the cost and schedule investment to meet testing requirements for such an evaluation.

5.11.2 LFT&E Report for Full-Rate Production Decision Review (FRP DR)*

[*fm SNI 5000.2D, 5.11.2: For programs involving covered major systems, major munitions or missiles, or product improvements (modifications) thereto, the DA shall submit a LFT&E report to DOT&E, via CNO (N091) or Director, MCOTEA, as appropriate. The submission shall allow DOT&E sufficient time to prepare an independent report and submit it to Congress prior to the program proceeding into FRP. PMs shall keep CNO (N091), apprised of the program's LFT&E progress and execution. See*

reference (b), enclosure 5, for implementation requirements for programs subject to LFT&E statutes.

**Not applicable to ACAT IA programs.*]

5.11.2.1 <u>LFT&E Waivers*</u>

[*fm SNI 5000.2D, 5.11.2.1: Request to waive full-up system-level live fire survivability and lethality testing must be submitted by USD(AT&L) for ACAT ID programs or ASN(RD&A) for ACAT IC programs and below and approved by DOT&E prior to entry into SDD. Waiver requests not approved prior to SDD require Congressional relief granted to SECDEF on a case-by-case basis. Waivers shall be coordinated with the program sponsor and CNO (N091) or Director, MCOTEA, as appropriate. Programs seeking LFT&E waivers must provide an alternate LFT&E strategy and plan that are acceptable to DOT&E.*

**Not applicable to ACAT IA programs*]

5.11.3 <u>Beyond Low-Rate Initial Production Report</u>

[*fm SNI 5000.2D, 5.11.3: ACAT I and IA programs and programs on the OSD T&E Oversight List designated by DOT&E, shall not proceed beyond LRIP until the DOT&E has submitted a written report to the Secretary of Defense and the Congress as required by 10 U.S.C. Section 2399. See reference (b), enclosure 5, for the beyond LRIP report for designated OSD T&E oversight programs.*]

5.11.4 <u>Director, Operational Test and Evaluation (DOT&E) Annual Report</u>

[*fm SNI 5000.2D, 5.11.4: DOT&E prepares an annual report of programs subject to OT&E on the OSD T&E Oversight List and all programs covered by live fire test and evaluation during the preceding fiscal year. The report covers basic program description, test and evaluation activity, and provides the Director's assessment of the T&E. CNO (N912) coordinates efforts to review and validate factual information to support DOT&E requests in the development of the report. DON acquisition and test agencies may be tasked by CNO (N912) to assist in this effort.*]

5.11.5 <u>Foreign Comparative Test Notification and Report to Congress</u>*

[*fm SNI 5000.2D, 5.11.5: Deputy Under Secretary of Defense Advanced Systems and Concepts (DUSD (AS&C)), shall notify Congress a minimum of 30 days prior to the commitment of funds for initiation of new foreign comparative test evaluations. See reference (b), enclosure 5, for implementation requirements for DON ACAT programs involved in foreign comparative testing.*]

*Not applicable to ACAT IA programs.

5.11.6 Electronic Warfare (EW) T&E Report

[***fm SNI 5000.2D, 5.11.6: See reference (b), enclosure 3, for implementation requirements for designated DON EW programs.***]

Attachment 2 of the annual Secretary of Defense Memorandum, Designation of Programs for OSD Test and Evaluation (T&E) Oversight, provides guidance on content required for the report for those programs designated on the list with Note 2.

Annex 5-A

Index of Test & Evaluation Strategy (TES)/Test & Evaluation Master Plan (TEMP) Signature Page Formats

TES/TEMP Cover Page Format for ACAT I/IA and all programs on OSD DOT&E Oversight List

TES/TEMP Cover Page Format for ACAT II programs

TES/TEMP Cover Page Format for ACAT III programs

TES/TEMP Cover Page Format for ACAT IV programs

TEMP Cover Page Format for Software Qualification Testing

TES/TEMP Cover Pages

TES/TEMP Cover Page Format For ACAT I/IA
[and Other OSD T&E Oversight Programs]

TEMP NO. [Insert TEIN] REV. _____ [AS APPLICABLE]
[PROGRAM TITLE]
Acquisition Category (ACAT) _____
Program Element No. _____
Project No. _____

SUBMITTED BY:

_____ _____
PROGRAM MANAGER DATE

CONCURRENCE:

_____ _____
SYSCOM COMMANDER/PEO/DRPM DATE

_____ _____
COMOPTEVFOR/DIR, MCOTEA DATE

_____ _____
PROGRAM/RESOURCE SPONSOR (Flag) DATE

APPROVED FOR NAVY or MARINE CORPS:

_____ _____
CNO (N091)(Navy Sponsored) DATE
ACMC (Marine Corps Sponsored)

_____ _____
ASN(RD&A) DATE

APPROVED:

_____ _____
COGNIZANT OIPT LEADER DATE

_____ _____
DOT&E DATE

Distribution statement per reference (v), Chapter 8, Exhibit 8A.
CLASSIFIED BY (see reference (v), Chapter 6):_____
REASON FOR:_____
DECLASSIFY ON:_____

TES/TEMP Cover Page Format For ACAT II Programs

TEMP NO. [Insert TEIN] REV. _____ [AS APPLICABLE]
[PROGRAM TITLE]
Acquisition Category (ACAT) II
Program Element No. _____
Project No. _____

SUBMITTED BY:

_____ _____
PROGRAM MANAGER DATE

CONCURRENCE:

_____ _____
SYSCOM COMMANDER/PEO/DRPM DATE

_____ _____
COMOPTEVFOR/DIR, MCOTEA DATE

_____ _____
PROGRAM/RESOURCE SPONSOR (Flag) DATE

APPROVED FOR NAVY or MARINE CORPS:

_____ _____
CNO (N091)(Navy Sponsored) DATE
ACMC (Marine Corps Sponsored)

_____ _____
ASN(RD&A) DATE

Distribution statement per reference (v), Chapter 8, Exhibit 8A.
CLASSIFIED BY (see reference (v), Chapter 6):_____
REASON FOR:_____
DECLASSIFY ON:_____

TES/TEMP Cover Page Format For ACAT III Programs

TEMP NO. [Insert TEIN] REV. ____ [AS APPLICABLE]
[PROGRAM TITLE]
Acquisition Category (ACAT) III
Program Element No. _____
Project No. _____

SUBMITTED BY:

_____ _____
PROGRAM MANAGER DATE

CONCURRENCE:

_____ _____
SYSCOM COMMANDER/PEO/DRPM DATE
(if ASN(RD&A) retains MDA)

_____ _____
COMOPTEVFOR/DIR, MCOTEA DATE

_____ _____
PROGRAM SPONSOR/CMC (DC,CD&I)(Flag) DATE

APPROVED FOR NAVY or MARINE CORPS:

_____ _____
CNO (N091), or designee (Navy Sponsored) DATE
ACMC, or designee (Marine Corps Sponsored)

_____ _____
MILESTONE DECISION AUTHORITY DATE

Distribution statement per reference (v), Chapter 8, Exhibit 8A.
CLASSIFIED BY (see reference (v), Chapter 6):_____
REASON FOR:_____
DECLASSIFY ON:_____

TES/TEMP Cover Page Format For ACAT IV Programs

TEMP NO. [Insert TEIN] REV. ____ [AS APPLICABLE]
[PROGRAM TITLE]
Acquisition Category (ACAT) IV
Program Element No. _____
Project No. _____

SUBMITTED BY:

_____ _____
PROGRAM MANAGER DATE

CONCURRENCE:

_____ _____
COMOPTEVFOR/DIR, MCOTEA DATE
[for ACAT IVT only]

APPROVED FOR NAVY or MARINE CORPS:

_____ _____
CNO (N091), or designee (Navy Sponsored) DATE
ACMC, or designee (Marine Corps Sponsored)
[for ACAT IVT only]

_____ _____
MILESTONE DECISION AUTHORITY DATE

Distribution statement per reference (v), Chapter 8, Exhibit 8A.
CLASSIFIED BY (see reference (v), Chapter 6):_____
REASON FOR:_____
DECLASSIFY ON:_____

TEMP Cover Page Format For
Software Qualification Testing Programs

TEMP NO. [Insert TEIN] REV. _____ [AS APPLICABLE]
SOFTWARE QUALIFICATION TESTING FOR
[PROGRAM TITLE]
Program Element No. _____
Project No. _____

SUBMITTED BY:

_____ _____
PROGRAM MANAGER DATE

CONCURRENCE:

_____ _____
COMOPTEVFOR/DIR, MCOTEA DATE

_____ _____
CNO (N091)/CMC (DC,CD&I) DATE

APPROVED:

_____ _____
SYSCOM COMMANDER/PEO/DRPM DATE

Distribution statement per reference (v), Chapter 8, Exhibit 8A.
CLASSIFIED BY (see reference (v), Chapter 6):_____
REASON FOR:_____
DECLASSIFY ON:_____

Annex 5-B

Fleet RDT&E Support Request

Request for:____ Quarter FY: ____ Date of Request: _____
Classification: _____
TEIN: _____
Title: _____
Code: (your office code)
Type: (DT&E/OT&E)_____ Phase:____
TEMP Signature Date:_____(*DD-MMM-YY*)
Fleet: (PAC/LANT)_____
Start Date: _____ (*DD-MMM-YY*) End Date: _____ (*DD-MMM-YY*)
Recommended Priority:_____ (1,2,3; DON GB, para 5.4.6.1.2)
Purpose of this phase of testing:_____
_____
_____
Support required: (use additional paragraphs if additional units are needed)

A. 1. Unit Type and Number Requested:_____
Special Equipment to be installed:_____
2. Unit's Scheduling Authority:_____
3. Test Location (OPAREA):_____
4. Level of Support:_____
(not-to-interfere, concurrent, dedicated; DON GB, para 5.4.6)
5. a. Preferred Dates Start: _____ (*DD-MMM-YY*) End: _____ (*DD-MMM-YY*)
Start No Later Than: _____ (*DD-MMM-YY*)
Complete No Later Than: _____ (*DD-MMM-YY*)
b. Number of Days on Station:_____ Hours/Day:_____
c. For Aircraft: A/C Sorties:_____ Hrs/Sortie:_____, and
Sorties/Day:_____
d. Minimum Times between Sorties/Test Periods:_____
6. Remarks: (See Notes)_____
_____
_____

B. 1. Unit Type and Number Requested:_____
Special Equipment to be installed:_____
2. Unit's Scheduling Authority:_____
3. Test Location (OPAREA): _____
4. Level of Support:_____
(not-to-interfere, concurrent, dedicated; DON GB, para 5.4.6)
5. a. Preferred Dates Start: _____ (*DD-MMM-YY*) End: _____ (*DD-MMM-YY*)
Start No Later Then: _____ (*DD-MMM-YY*)
Complete No Later Then: _____ (*DD-MMM-YY*)
b. Number of Days on Station:_____ Hours/Day:_____
c. For Aircraft: A/C Sorties:_____ Hrs/Sortie:_____
Sorties/Day:_____
d. Minimum Times between Sorties/Test Periods:_____
6. Remarks: (See Notes)_____
_____
_____

C. 1. Unit Type and Number Requested:_____
Special Equipment to be installed:_____
2. Unit's Scheduling Authority:_____
3. Test Location (OPAREA):_____
4. Level of Support:_____
(not-to-interfere, concurrent, dedicated; DON GB, para 5.4.6)
5. a. Preferred Dates Start: _____ (*DD-MMM-YY*) End: _____ (*DD-MMM-YY*)
Start No Later Than: _____ (*DD-MMM-YY*)
Complete No Later Than: _____ (*DD-MMM-YY*)
b. Number of Days on Station:_____ Hours/Day:_____
c. For Aircraft: A/C Sorties:_____ Hrs/Sortie:_____ , and
Sorties/Day:_____
d. Minimum Times between Sorties/Test Periods:_____
6. Remarks: (See Notes)_____
_____
_____

(Name; Command; email; Voice and Fax Phone Numbers, DSN and Commercial)
POC:
OTD:
DT&E
Coord:
OTC:
Program Sponsor:

NOTES:

1. Requests should be as general as possible to allow the schedulers flexibility.
2. Include a list of ships that have the correct equipment configuration installed to support the tests.
3. Designate unique fleet personnel support requirements (e.g.: SEAL Teams, ULQ13 Van/Crew).
4. Service request remarks: State time required to install and remove equipment and by whom. Address the following questions:
   a. Can it be installed pierside (drydock/SRA/ROH)?
   b. Has equipment installation been approved? By whom?
   c. Will installation affect unit operation or other equipment onboard?
   d. Is any crew training required?
   e. How many riders are required to embark (keep to a minimum)?
   f. If more than one unit is required, state which units must work together and the minimum concurrent time.
5. Address impact on program if services are not filled such as:
   a. Loss of programmed monies (specify amount).
   b. Increased cost due to delay (specify amount).
   c. Impact on related joint programs or operations.
   d. Congressional and or/OSD interest or direction.
   e. Unique factors:
      (1) Deployment schedule of test asset.
      (2) Overhaul schedule.
      (3) "One-of-a-kind" underway events required for testing.
   f. Delay in projected production and cost to Navy.

Annex 5-C

Test and Evaluation Identification Number Request Format

3960
Ser
(DATE)

From: (Program Office)
To: Chief of Naval Operations (N912)
Via: (Sponsor)

Subj: REQUEST FOR TEST AND EVALUATION IDENTIFICATION NUMBER (TEIN) ASSIGNMENT FOR (PROGRAM NAME)

Ref: (a) SECNAVINST 5000.2D
(b) Initial Capabilities Document for (Program Name) of (Approved Date)

1. Per reference (a), request a Test and Evaluation Identification Number (TEIN) be assigned to the (Program Name), (Program Element Number; Project Number).
(Add 2-3 sentences describing purpose of program) This ACAT (ACAT level) program is being developed to meet the requirements of reference (b).

2. Points of contact are:

Responsibility	Name	Code	Telephone
Program Manager	(Program Manager)		
Requirements Officer	(OPNAV Sponsor)		
T&E Coordinator	(N912 point of contact)		

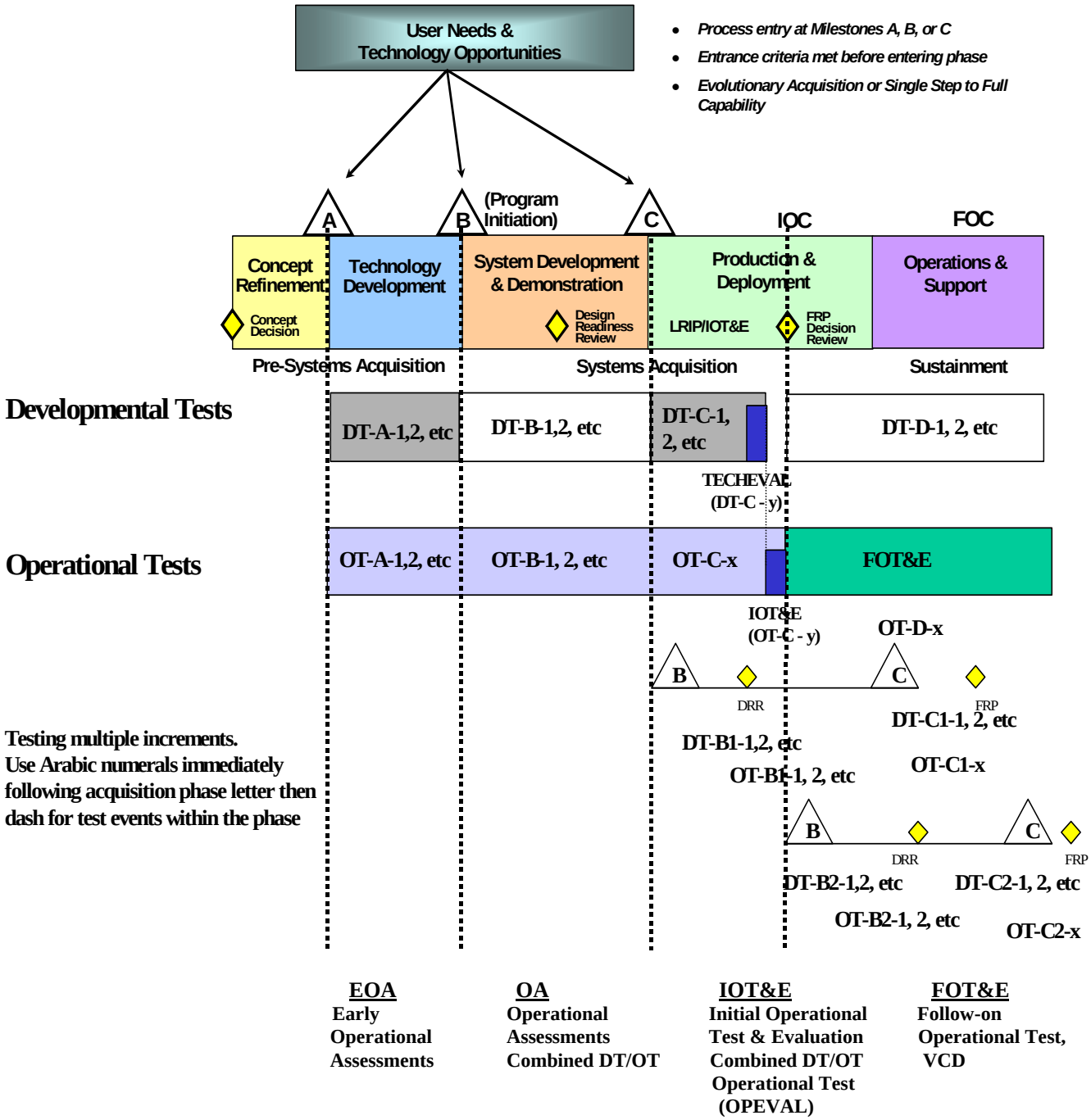
3. Milestone Status: (indicate dates milestones were achieved and planned dates for future milestones)

(Program Manager Signature)

Copy to:
COMOPTEVFOR (01B6)
(Additional Office codes if necessary)

Annex 5-D

Notional Schedule of Test Phases in the Acquisition Model



Annex 5-E

Navy Certification of Readiness for OT Message Content

The message certifying a system's readiness for OT&E should contain the following information:

1. Name of the system

2. OT-[phase]

3. TEMP [number]

4. TEMP approval date

5. For software testing, identify the specific release to be tested.

6. Waivers (identify criteria in SECNAVINST 5000.2D to be waived, if any; if none, state "none"). (SECNAVINST 5000.2D should be Ref A of the certification message)

7. State projected limitations that waived criteria will place on upcoming operational testing.

8. Deferrals (identify deferrals from a testing requirement directed in the TEMP; if none, state "none".). (The TEMP should be Ref B of the certification message)

9. State projected limitations that waived TEMP requirement will place on upcoming operational testing.

10. State potential waiver impact on fleet use.

11. State when waived requirement will be available for subsequent operational testing.

12. Additional remarks.

A format for the Navy Certification of Readiness for Operational Test and Evaluation message is provided on the following page.

Navy Developing Activity Certification Message Format

FM [Developing Activity (DA)]
TO CNO WASHINGTON DC//N091//

INFO COMOPTEVFOR NORFOLK VA//00//
SECDEF WASHINGTON DC//DOT&E/DT&E//(if on OSD oversight list)
[**info other commands as appropriate]**
[Classification]//N05000//
MSGID/GENAMDIN/**[DA]**/**(Code)**//
SUBJ/ **[Program Name]** CERTIFICATION OF READINESS FOR OPERATIONAL TEST AND EVALUATION (OT-**XXX**), CNO PROJECT **xxxx**//
REF/A/DOC/SECNAVINST 5000.2D/date//
REF/B/DOC/TEMP **xxxx**/**(date)**//
[Other references as appropriate]
NARR/REF A IS A SECNAVINST FOR IMPLEMENTATION OF OPERATION OF THE DEFENSE ACQUISITION SYSTEM AND THE JOINT CAPABILITIES INTEGRATION AND DEVELOPMENT SYSTEM. REF B IS THE **[Program Name]** TEST AND EVALUATION MASTER PLAN NO. **xxxx** APPROVED ON **[date]**.//
POC/**[Name]**/**[Program Office Code]**/-/-/TEL:COM**(xxx)xxx-xxxx**/TEL:DSN **xxx-xxxx**//
RMKS/1. IAW REF A, THIS MESSAGE CERTIFIES THAT THE **[Program Name], (for software testing identify the specific release to be tested during OT&E)** IS READY FOR OPERATIONAL TEST (OT-**xxx**) AS OUTLINED IN REF B.
2. WAIVERS TO THE CRITERIA OF REF A ARE REQUESTED FOR:
A: **[Identify Ref A, enclosure (5), para 5.6.1, criteria to be waived, if any; if none, so state.**

(1) (Limitation that waived criteria will place on upcoming operational testing.]

[Repeat above format for each criteria requested for waiver.]

3. DEFERRALS TO TESTING SYSTEM CAPABILITIES/REQUIREMENTS OF REF B:
A: **[State requested deviation from a testing requirement directed in Ref B TEMP. Cite specific critical operational issues (COIs) in Ref B; if none, so state.]**

(1) [Limitations that deferred TEMP requirement will place on upcoming operational testing.]
(2) [Potential impacts on fleet use.]
(3) [State when deferred requirement will be available for subsequent operational testing.]

[Repeat above format for each TEMP requirement requested for deferral.]

4. [Additional remarks as appropriate.]
A: **[State any other issues that may impact the test, such as limited resources or timing constraints for testing.]**

BT

Annex 5-F

Elements of Risk Assessment for Software Intensive System Increments

There are two primary factors in assessing the risk of a system element: the likelihood of failure and the impact on the mission of an increment's failure to be operationally effective and suitable. Fortunately, these two components need to be evaluated only to the degree required to decide among a few distinct levels of operational testing.

This appendix will discuss these two fundamental elements of risk assessment: the likelihood of failure, which will be evaluated via a surrogate method, and the mission impact of failure, which will be approached in a more direct fashion. The final step is the fusion of these two evaluations into an assessment of the overall risk of a system increment. This document was developed to present a general concept and suggestions for tailoring operational testing to risk. Users should recognize that the procedures needed to properly assess risk should be tailored to the characteristics of the specific increment. The procedures presented in this annex are provided as examples to guide the OTA in the risk assessment process, rather than a checklist or hard set of rules.

1.1 Identification and Evaluation of Threats to Success for Software Intensive System Increments

The data required to accurately define the true probability of failure of an increment are not likely to be available. As an alternative approach, the analysis can be based upon an evaluation of a comprehensive set of factors that have been shown as potential threats to the success of a software-intensive increment. These threats to success can be evaluated relative to the specific increment, and a general estimate of potential effects can be determined. The evaluation of the cumulative effect of the threats to an increment's success is analogous to determining the likelihood of failure for the increment. Of necessity, this aggregate assessment is usually a judgment call.

Most concerns associated with the deployment of a new, generic, software-intensive system increment may be grouped under a few general categories. This annex identifies six primary categories of threats to success, although fewer or more categories may be appropriate for a specific increment. This set of categories is certainly not unique, and any set that comprehensively covers the issues of concern will give similar structure to the approach. Further, the categories may have significantly different relative sensitivities for any particular increment. The six categories of threats to success presented as examples are:

1. Development
2. Implementation
3. Technology
4. Complexity
5. Safety
6. Security

The OTA should first assess the threat to an increment's success from each separate area, by examining the particular characteristics of the increment and its development. This evaluation is guided by the specific issues identified with each category and based upon input from the user, the developer, the developmental tester, the post-deployment software support organization, available documentation, and any new data collected by the OTA. Clearly, not all issues within a category will have equal importance.

Then, based upon these assessments and the relative significance of each area, the OTA should make an overall evaluation of the likelihood of the increment's failure to be operationally effective and suitable. Not all categories need to be given equal importance. The evaluator should base this judgment upon the particulars of the increment, the development process, and the utility and reliability of available data. Note that the categories and issues presented are merely examples; the evaluator should always consider risk factors specific to the increment. In other words, use good judgment, based on detailed knowledge of the increment.

Each category should be evaluated as accurately as possible, at least to the levels of resolution described below. Each of these levels is defined in terms of typical characteristics; actual assessments will be a mix of positive, neutral, and negative characteristics.

1. Insignificant Threat to Success (Insignificant Likelihood of Failure) – Increments posing this level of threat to success are typically small, simple, modular increments that come from a highly reliable developer and an ideal development environment. Additional characteristics that support this assessment are a program's demonstrated success with all previous increments, employment of very mature technologies, excellent training programs or highly experienced users, no impact upon other system elements, and no safety or security issues.

2. Low Threat to Success (Low Likelihood of Failure) – Increments posing this level of threat to success may be small-to-medium-sized, involving few complicated issues. Other characteristics justifying a low threat to success are a solid development environment with few shortcomings, employment of stable technologies, capable users, little interaction with basic system elements, and few safety or security issues.

3. Moderate Threat to Success (Moderate Likelihood of Failure) – This level of threat to success is typically assigned to medium- to large-sized increments having several complex elements and employing recent technological developments. Complicated interfaces, significant interaction with external system resources, or multiple safety and security concerns would suggest this level of assessment.

4. High Threat to Success (High Likelihood of Failure) – This highest level of threat to success typically involves large to very large, complex, multi-functional increments. Other characteristics include untested or unreliable development environments with poor performance histories, new technologies, many untested interfaces, new or untrained users, and multiple safety and security issues.

It is unlikely that all six categories of evaluation will be assigned the same level of threat to success. One simple scheme of evaluation would be to assign to the increment as a whole a level equal to or greater than the highest level of threat to success determined for any single category. For example, if the highest level category poses a moderate threat to success, then the overall level should be no lower than moderate. If two or more important categories are rated as moderate, then the overall level might be elevated to a high threat to success (or high likelihood of failure).

Example Issues for Evaluating Threats to Success

The following issues represent some potential threats to an increment’s success. Detailed knowledge of a particular system increment will tailor the assessment.

1. Development

a. Have capabilities been adequately described and user requirements clearly identified?

b. Do the capabilities/requirements address operational needs rather than specifying a technical solution?

c. Are the capabilities included in the new increment traceable to requirements, as specified in the requirements traceability matrix?

d. What is the developer's Capability Maturity Model rating as defined by the Software Engineering Institute? Is the rating justified by the developer's experience?

e. How extensive was the developmental test program for this increment, i.e., did the developmental testing (DT) program explicitly address each capability/requirement? Did the DT program also evaluate operational capabilities/requirements?

f. Does the developer employ a robust set of software management indicators?

g. Are interfaces with existing systems fully documented and under configuration control?

h. Does the developing contractor’s test agent have sufficient experience and technical expertise to conduct a proper technical evaluation?

i. Has the necessary integration and regression testing been conducted?

j. Were any Priority l or Priority 2 problems (as defined in IEEE/EIA Standard 12207.2-1997, Annex J) experienced with the last increment from this development team?

k. How numerous and how significant are the deficiencies identified in previous tests of the new increment?

l. What is the history of the developer regarding similar programs?

m. What is the history of the developer with respect to previous increments?

n. How effective is the established configuration management process for the program development and/or installed systems?

o. How extensively have prototypes been used to evaluate acceptance by typical users?

p. Have exit criteria been identified for developmental testing of this increment?

q. Are there requirements/capabilities of this increment that will be unavailable for testing?

2. Implementation

a. User:

(1) Is the user committed to the successful implementation of the new increment?

(2) Have operational and user support procedures been developed and readied for implementation along with the new increment? Have user representatives developed appropriate concepts of operations, policies, procedures, training, support, and contingency plans for a full operational deployment?

(3) Do the operators possess the skill levels required to use the increment's capabilities effectively?

(4) Has an adequate training plan been developed or implemented to include reorientation and sustainment training?

(5) Has a point of contact been established to represent the views of users?

b. Organization:

(1) Is the receiving organization committed to the successful implementation of the new increment?

(2) Is the receiving organization prepared for the changes in business processes associated with the new increment?

(3) Have new standard operating policies and procedures been developed or implemented to use the capabilities of the new increment?

(4) Has the receiving organization developed plans for continuity of operations during the installation of the new increment?

3. Technology

a. How dependent is the new increment upon new technologies (hardware and software)?

b. What is the commercial tempo of change in the technology areas represented in the increment?

c. How mature are the new technologies incorporated into the increment?

d. Does the new increment introduce any new standards or protocols?

e. Does the integration of the entire system (e.g., hardware, software, communications, facilities, management, operations, sustainment, personnel) present unusual challenges?

f. Does the system include the necessary system administration capabilities?

g. If the increment is primarily COTS, NDI, or GOTS (government-off-the-shelf), what is the past performance and reliability?

h. For new technologies, what is the performance record in other applications?

4. Complexity

a. How complex is the new increment (e.g., industry standard complexity metrics, or as compared to other fielded increments)?

b. How many agents (government, contractors, sub-contractors) participated in the development of this increment?

c. How stable are the system requirements?

d. What is the proportional change to system hardware and software introduced by the new increment?

e. What is the cumulative change to system hardware and software since the last full operational test?

f. Is the new system (including the increment of interest) to be integrated with other systems during development or deployment?

g. How complex are the external system interface changes (hardware, software, data) in the new increment?

h. How complex or intuitive are the user interfaces with the new increment?

i. How complex are the interactions of the new increment with the fielded databases?

j. To what extent does the new increment introduce changes that place in jeopardy or modify the system data structures?

k. Does the new increment implement a change in executive software (operating system or database management system)?

l. How complex/stable are the automated features in the new increment?

5. Safety

a. Does the system present any safety hazards to the operators or operational environment?

6. Security

a. Does this system require multi-level security?

b. Can the new increment affect the security or vulnerability (to information warfare) of the installed system (e.g., have external interfaces been added)?

c. Does the new increment modify or possibly interfere with information assurance protective measures?

d. If it has external interfaces, has the system been tested for unauthorized access?

In addition to the above general matters, there may be other overriding concerns – conditions that are potentially so important that, if they are present, a thorough and comprehensive operational testing effort is mandatory.

1.2 Identification and Evaluation of Mission Impact of Increment Failure

The mission impact assessment should consider the impact of the possible failure of the new increment on the mission of the whole system. This assessment should also consider increment-related changes in concept of operations, maintenance concept, training concept, and the roles of the increment in a possible SoS configuration. Table F-l provides a typical set of potential mission impact assessments, related to resolution of system COIs.

Table 5-F-1. Degree of Mission Impact

Effect on Mission	**Definition**
Minor Impact	Increment failure would cause noticeable problems but no major interference with mission accomplishment. System COIs can be satisfactorily resolved, even without increment success.
Moderate Impact	Increment failure could cause substantial degradation of mission-related capabilities. System COIs are moderately dependent upon increment performance.
Major Impact	Element is required for mission success. System COIs are critically dependent upon increment performance.
Catastrophic Impact	The element is required for mission success, and its malfunction could cause significant damage to the installed system, to other interconnected systems, or to personnel.

The evaluator must make a mission impact assessment for each of the mission areas affected by the new increment. The total impact to the mission is then assessed as the highest impact noted for any area of concern, or at a level above the highest level noted if many lower potential impacts are evident.

1.3 Assessing the Risk of a Software Intensive System Increment

When the mission impact and likelihood of failure of an increment have been determined, the risk assessment may be made as the product of these two basic elements. However, in assessing risk, the mission impact should be weighted more heavily than the likelihood of failure. The methodology in Annex 5-G presents a direct method for determining the proper level of OT from the levels of mission impact and likelihood of failure obtained from the analysis in Annex 5-F.

Annex 5-G

Determining Appropriate OT&E for Software Intensive System Increments

The specific evaluation procedures presented in this annex are provided as examples, rather than requirements.

1.1 Multiple Levels of OT&E for Software Intensive System Increments

The tester must determine the level of OT that most effectively provides "affordable confidence" that an increment will meet mission needs. A range of test activities should be considered and matched to the risk of the specific system increment. The range of OT for increments other than the core increment extends through four levels, from an abbreviated assessment to a full, conventional OT&E.

For each of these four levels of OT&E, it is presumed that the exit criteria from DT have been satisfied and that all previously deployed increments are functioning properly prior to the fielding of any new increment. It is further presumed that user representatives have developed appropriate concepts of operations, policies, procedures, training, support, and contingency plans for a full operational deployment. Where these are lacking, the OTA must consider associated risk factors as high, increasing the level of OT required. Regardless of the level of testing actually executed, the OTA is obligated to implement applicable OSD policies in the course of testing such as the DOT&E policy regarding information assurance.

The detailed design of testing activities at each level of testing must be based upon the fundamental objective of evaluating the ability of the tested system to accomplish its mission goals when deployed. The increment’s mission goals are expressed in the measures of effectiveness and suitability and the COIs stated in the TEMP.

Level I Test – After complete and successful developmental testing, permit limited fielding and assess feedback from the field (by the OTA) prior to full fielding. Contractor presence is permitted during the Level I test. Plans for recovery from failures, prepared by the Program Management Office (PMO) and validated by the OTA, must be in place prior to limited fielding.

Level I testing is appropriate for maintenance upgrades and increments that provide only minor system enhancements, pose an insignificant risk, and can be easily and quickly removed. Increments judged to be of sufficiently low risk for Level I testing will usually be delegated to the Component for testing, evaluation, and fielding decisions. The OTA prepares an assessment to support any fielding decision. A copy of the

assessment is to be provided to DOT&E. Key features of Level I testing are:

1. It is essentially a DT effort.

2. The OTA monitors selected developmental/technical testing activities.

3. Limited fielding is permitted prior to the OTA evaluation.

4. The OTA prepares an assessment to support a fielding decision by the MDA.

Level II Test – Assessment performed by an OTA primarily using DT data and independent "over-the-shoulder" observations. The OTA may prescribe and observe operationally realistic test scenarios in conjunction with DT activities. Contractor presence is permitted during the Level II test. DOT&E may observe any OT activity.

Level II testing should be applied to increments that provide only minor system improvements and present a minor risk. Such lower risk increments have only minimal potential to impact other system applications and cannot disrupt the basic system's ability to support the mission. After thorough Level II testing, an increment may be deployed to selected operational sites for additional feedback (collected by the OTA) if needed prior to full fielding. Features of the Level II test are:

1. It is essentially a combined DT/OT testing effort.

2. The assessment is based primarily upon close monitoring of selected developmental/technical activities and upon DT results.

3. Prior to the limited fielding, plans must be in place for recovery from failures.

4. The OTA evaluates the limited fielding results and reports on the operational effectiveness and suitability to the AE to support a fielding decision by the MDA.

5. A copy of the evaluation report is provided to N091.

Level III Test – OTA personnel coordinate the Level III test (which is carried out by user personnel in an operational environment) and evaluate the operational effectiveness and suitability using primarily independently collected OT data. The Level III Test is conducted at one or more operational sites. In addition to normal user operations, the OTA may prescribe that scripted test events be executed and observed. Level III testing may be conducted in two phases. The PMO controls Phase I, allowing contractors to fine-tune the system, but the OTA

supervises Phase II, which defines an operational period without PMO or contractor participation. OT evaluators are allowed during both phases.

The Level III Test is suitable for increments supporting modest, self-contained, system improvements that present a moderate level of risk, but are limited in the potential disruption to an installed system. Features of Level III testing are:

1. Actual operators are at the operational site(s) performing real tasks.

2. The emphasis is on assessment and evaluation.

3. It is less formal than a full OT.

4. Prior to fielding, plans are in place for recovery in the event of failure.

5. The OTA prepares an evaluation of operational effectiveness and suitability for the AE.

6. A copy of the evaluation report is provided to N091.

Level IV Test – Determine the operational effectiveness and suitability of a new increment by evaluating affected COIs under full OT constraints. This is the highest level of operational test and the most comprehensive. The OTA carries out test events in an operational environment. The OTA evaluates and reports on the operational effectiveness and suitability of a new system increment based upon all available data, especially independently collected OT data. In special cases, the verification of minor capabilities and secondary issues may be relegated to lower levels of testing. Level IV testing must comply with all provisions of the DOD 5000 series regulations.

1.2 Matching OT&E to Risk Assessment

The OT&E Action Determination Matrix shown in Table 5-G-1 forms the basis for relating the assessed failure potential (threat to success) and mission impact to an appropriate level of OT&E. The matrix provides for the four levels of OT&E described in the last section.

Table 5-G-1. OT&E Action Determination Matrix

	Effect on Mission			
Failure Potential	**Minor Impact**	**Moderate Impact**	**Major Impact**	**Catastrophic Impact**
Insignificant	I	I-II	II-III	III-IV
Low	I-II	II-III	III-IV	IV
Moderate	II-III	III-IV	III-IV	IV
High	III-IV	III-IV	IV	IV

Annex 5-H

Software Intensive System Responsibilities for and Schedule of OT&E Actions

1.1 Responsibilities

1. Operational Test Agency – With regard to the OT&E for a follow-on system increment, the OTA is responsible for: Determining the type of data and level of detail required for assessing the threats to increment success. This includes:

a. Collecting and analyzing information concerning potential threats to the success of the system increment, and determining the likelihood of failure based upon those threats.

b. Determining the type of data and level of detail required for assessing the potential mission impact of the failure of a system increment.

c. Collecting, analyzing, and determining the potential mission impacts associated with the system increment.

d. Determining an appropriate level of OT&E according to the risk assessment.

e. Developing and coordinating the applicable level of operational test plans.

f. Validating recovery plans prior to deployment of an increment to any operational test sites.

g. Conducting the approved level of OT&E.

h. Developing the applicable independent evaluation report and providing it to the appropriate organizations.

i. Making operational effectiveness and suitability recommendations.

2. Program Management Office – The PMO is responsible for:

a. Providing the programmatic data required to evaluate threats to the success of the new increment to the OTA action officer and user representative.

b. Providing the technical information requested to support the evaluation of each significant threat to the increment’s success.

c. Developing recovery plans prior to fielding of an increment to any operational test sites.

d. Certifying the increment's readiness for OT&E.

3. User – The user (or user representative) is responsible for:

a. Participating in the planning and execution of the OT&E.

b. Providing the OTA with information regarding mission impacts of increment failure.

c. Assisting the PMO in developing recovery plans, including workarounds for possible increment malfunctions.

4. Director, Test and Evaluation and Technology Requirements (N091) – for Navy programs, N091 is responsible for:

a. Providing guidance as needed in the preparation of risk assessments and determining the appropriate level of OT.

b. Evaluating and responding to the test and evaluation master plan (TEMP) and approving if appropriate.

c. Evaluating and responding to adequacy of the operational test plan when appropriate.

d. Resolve issues between the DA and OTA.

1.2 Schedule Of Activities

Table H-1 shows key OT activities, schedules, and responsibilities.

Table 5-H-1. Operational Testing Actions, Schedules, and Responsibilities

Action	When	Respon-sible Agency	Comments
Prepare Program Risk Assessment	As soon as data becomes available	OTA	OTA and PM conduct assessments with information provided by PM and with participation of user and other appropriate Component agencies
Determine Level of Operational Test	Upon completion of risk assessment	OTA	Based on risk assessment
Develop Operational Test Plan	Upon decision regarding level of OT	OTA	Brief elements within Navy/Marine Corps, as required
Complete Operational Test Plan	Submit 30 days prior to start of OT	OTA	Brief elements within Navy/Marine Corps, as required (Following this stage, the PM or PEO will need to certify that the increment is ready for operational testers to begin evaluation at the appropriate level.)
Conduct Operational Test		OTA	
Analyze Test Results and Prepare Report	Complete within 60 days of test completion	OTA	OTA briefs PM, plus other stakeholders as required, on test results
Prepare and Present Deployment Recommendations to MDA		OTA	

Chapter 6
Resource Estimation

References: (a) DOD Instruction 5000.02, Operation of the Defense Acquisition System, of 8 Dec 08
(b) USD(P&R) Memorandum, Interim Policy and Procedures for Strategic Manpower Planning and Development of Manpower Estimates, of 10 Dec 03

6.1 Resource Estimates

6.1.1 Life-Cycle Cost Estimates

The Naval Center for Cost Analysis (NCCA), Assistant Secretary of the Navy (Financial Management and Comptroller) (ASN(FM&C)), Office of Budget, Financial Management Branch (FMB)-6, has promulgated guidance for formal reviews of Milestones B and C life-cycle cost estimates and component cost analyses for Department of the Navy (DON) Acquisition Category (ACAT) IC, IAC, and IAM programs. Estimates are prepared by program offices and, independently, by NCCA. Each review is chaired by the Director, NCCA, and is referred to as the "DON Cost Analysis Improvement Group (CAIG)." Guidance for reviews is available on NCCA's website under the title "DON CAIG Instruction (SECNAVINST 5420.196)."

http://www.ncca.navy.mil/resources/guidance.cfm.

Further, NCCA has also established guidelines for developing thorough, complete documentation for life-cycle cost estimates for weapon systems and automated information systems. This guidance, applicable to both Independent life-cycle Cost Estimates (ICEs), component cost analyses, and program-office life-cycle cost estimates, is also available on the above website under the title "NCADINST 4451.1A, Guide for the Documentation of Independent Cost Estimates."

6.1.2 Cost Analysis Requirements Description (CARD)

A sound cost estimate is based on a well-defined program. For ACAT I, IA, and II programs, the CARD is used to formally describe the acquisition program (and the system itself) for purposes of preparing both the program office cost estimate (and the DoD Component cost position, if applicable) and the Office of the Secretary of Defense (OSD) CAIG independent cost estimate. Reference (a), enclosure 4, specifies that for major defense acquisition programs, the CARD will be provided in support of major milestone decision points (Milestone B, Milestone C, and the Full-Rate Production Decision Review (FRP DR)). In addition, for major automated information system programs, the CARD is prepared whenever an Economic Analysis is required. The CARD is prepared by the program office and approved by the Department of

Defense (DoD) Component Program Executive Officer (PEO). For joint programs, the CARD includes the common program agreed to by all participating DoD Components as well as all unique program requirements of the participating DoD Components. DoD 5000.4-M, *DoD Cost Analysis Guidance and Procedures*, Chapter 1, provides further guidelines for the participation of the CARD.

6.1.3 Manpower Estimates

[***fm SNI 5000.2D, 6.1.3: Manpower estimates are required by statute for ACAT I programs. Manpower estimates shall also be developed for other ACAT programs that are manpower significant at the request of the Component manpower authority per reference (b). CNO (N12) and CMC (Deputy Commandant, Manpower and Reserve Affairs (DC,M&RA)) are the designated Navy and Marine Corps Component manpower authorities, respectively. For ACAT ID programs, CNO (N12)/CMC (DC,M&RA) shall forward approved*** **manpower estimates** ***to the office of the Under Secretary of Defense (Personnel and Readiness).***]

Manpower Estimates (MEs) are one of the key documents of human systems integration. MEs are a source for out-year projections of military and civilian manpower and contract support required for the acquisition and upgrade of weapon, support and automated information systems. MEs are required by 10 U.S.C. Section 2434. Development of the manpower estimate is the responsibility of the resource sponsor. MEs may be requested by CNO (N12)/CMC (DC,M&RA) for other selected programs. The initial ME is required at MS B with an update at MS C and FRP DR. MEs should include a target audience description (TAD) that provides information about the personnel that will use, operate, maintain, train and repair a system. The TAD may consist of military personnel, civilians and/or contractors, or a mix thereof. If it is a joint service system, members of the other branches of service should also be identified and included as a part of the TAD. The TAD provides a description of the quantity, qualifications, and characteristics of the personnel who will operate, maintain and support the system. The TAD also is the baseline for the Training System Plan and Affordability Assessment, as well as providing a baseline for design trade-offs.

6.1.3.1 Manpower Considerations

The PM should determine and document manpower by rate and rating for both peacetime and wartime requirements. The PM should further identify specific vital objectives, and establish manpower authorization minimums necessary to achieve these objectives. CNO (N1) assistance may be used in developing manpower life-cycle cost estimates for ACAT II, III, and IV programs, if requested by the milestone decision authority (MDA) or the resource sponsor.

6.2 Affordability

6.3 Contract Management Reports

6.3.1 Contractor Cost Data Reporting (CCDR) for Hardware and Software –- (DID DI-FNCL-81565B/81566B/81567B) and Software Resources Data Report (SRDR) –- (DID DI-MGMT-81739/81740)

6.3.2 Contract Performance Report (CPR) -- (DID DI-MGMT-81466)

6.3.3 Integrated Master Schedule (IMS) -- (DID DI-MGMT-81650)

6.3.4 Contract Funds Status Report (CFSR) – (DID DI-MGMT-81468)

6.4 Analysis of Alternatives (AoA)

[*fm SNI 5000.2D, 6.4: The Gate 1 and Gate 2 processes of enclosure (2), paragraphs 2.11.4.1.1.1 (Gate 1) and 2.11.4.1.1.2 (Gate 2) amplify the AoA processes defined below and the guidance in DON Acquisition and Capabilities Guidebook, paragraph 6.4.*]

After an Initial Capabilities Document (ICD) is approved and validated, a Concept Decision (CD) is made to address the capability gaps identified. The incorporation of concepts discussed in the ICD, as well as those developed from related System of Systems (SoS) or Family of Systems (FoS), require additional analysis and refinement to ensure sufficient mission capability and economic benefit is achieved from any potential materiel solutions.

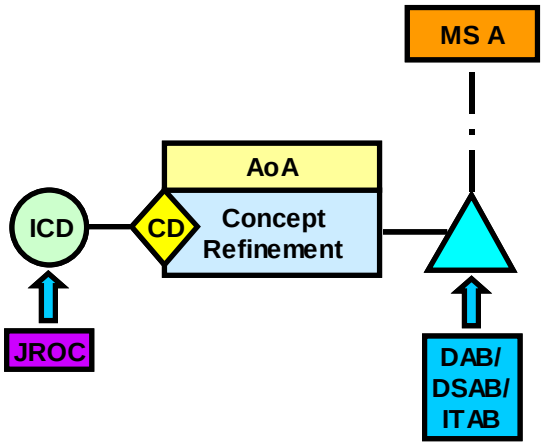


Figure 6-1. AoA and the JCIDS/Acquisition Process

All DON ACAT-level programs require the completion of an AoA prior to program initiation. Typically, this is in direct support of a Milestone A decision, as shown above, but in certain circumstances the MDA can direct additional reviews of alternatives leading to a Milestone B or C decision. AoAs must therefore be tailored to the scope, increment, phase, and potential ACAT-level of the individual programs they support.

Per reference (a), all ACAT I programs will receive initial guidance from the Office of the Secretary of Defense (OSD) Director, Program Analysis and Evaluation (PA&E) as part of the approval process leading to the CD. All DON ACAT I programs must incorporate this overarching guidance as part of their AoA plan. Programs designated ACAT II or below may begin AoA planning immediately.

For joint ACAT-level programs in which DON has been designate the Lead Service, AoA procedures should be tailored to include other Service representatives and approval authorities. In addition, consideration should be given towards the possibility of including international collaboration and acquisition options when appropriate.

Once completed, the AoA aids decision-making in establishing initial system performance thresholds and objectives, identifies cost and performance trade-offs, and highlights the analytical underpinnings for a multitude of program decisions. In general, the AoA provides a structured review and documentation of the alternatives, assumptions, and conclusions supporting the rationale for proceeding to a materiel solution.

6.4.1 Weapon System AoA

1. All DON weapon systems, regardless of ACAT level, must complete an AoA prior to program initiation. Per reference (a), program initiation normally occurs at Milestone B, but may occur at other milestones/decision points depending upon technology maturity and risk. At program initiation, a program must be fully funded across the Future Years Defense Program (FYDP) as a result of the Program Objectives Memorandum (POM)/budget process. That is, the program must have an approved resource stream across a typical defense program cycle (e.g., Fiscal Year (FY) 2006-2011). Concept Refinement (CR) and Technology Development (TD) phases are typically not fully-funded and thus do not constitute program initiation of a new acquisition program in the sense of reference (a).

2. Reference (a), enclosure 4, Table 3 directs multiple AoA reviews for all ACAT I programs as follows: Milestone A, Milestone B (update as necessary), and Milestone C (update as

necessary). The final report should discuss steps taken to ensure compliance with the Clinger-Cohen Act for weapon systems that are National Security Systems.

3. AoAs differ at each milestone, if prepared.

a. At Milestone A, the analysis focuses on broad tradeoffs available between a large range of different concepts. The analysis normally presents a "Go/No Go" recommendation. It demonstrates why a new system is better than upgrading/modifying an existing system. Cost estimates may be only a rough order of magnitude but, nevertheless, an estimate is required. A Milestone A AoA helps the MDA choose a preferred system concept and decide whether the cost and performance of the concept warrants initiating an acquisition program. These types of analyses also illuminate the concept's cost and performance drivers and key tradeoff opportunities; and provide the basis for the establishment of operational performance thresholds and objectives used in the Capability Development Document (CDD), Acquisition Program Baseline (APB), and Test and Evaluation Master Plan (TEMP).

b. At Milestone B, the analysis is more focused. Hardware alternatives present a narrower range of choices. The analysis is more detailed and contains more defined cost data. Point estimates are given with uncertainty ranges. Life-cycle costs are normally presented.

c. At production approval (Milestone C), the AoA, if required, is normally an update of the Milestone B document. It highlights any trade-off or cost changes. However, since cost and performance issues have typically been resolved prior to Milestone C, an AoA is not often required to support this milestone.

4. If the AoA is to be supplemented by another Service developed analysis, the director of the AoA should ensure that the assumptions and methodologies used are consistent for both Services.

5. See Annex 6-A for AoA preparation and processing procedures.

6.4.2 <u>IT AoA</u>

1. AoAs involving automated information systems are basically the same as discussed above; however, they must be constructed in a way that clearly demonstrates full compliance with all requirements discussed in reference (a) and enclosure (4) of this guidebook.

2. The final report should discuss steps taken to ensure compliance with the Clinger-Cohen Act and Financial Management Enterprise Architectures.

3. Reference (a), enclosure 4, Table 3 directs multiple AoA reviews for all ACAT IA major automated information systems as follows: Milestone A, Milestone B (update as necessary), Milestone C (update as necessary) and Full Deployment Decision Review (for AIS).

4. See Annex 6-A for AoA preparation and processing procedures.

6.5 Cost as an Independent Variable (CAIV)

CAIV should account for the cost of Manpower, Personnel, and Training (MPT). As part of CAIV, the PM should explore options that maximize use of technology to reduce MPT requirements. CAIV planning should account for the cost and risk of final disposal, with particular reference to hazardous materials. Requirements for product reclamation and recycling should be included. CAIV analyses should consider hazardous material management, disassembly, disposal, and reuse or resale of recovered materials.

6.5.1 Cost/Schedule/Performance Tradeoffs

For those programs that are part of a SoS or FoS, cost-performance tradeoffs should be performed in the context of an individual system executing one or more mission capabilities of the SoS or FoS.

Annex 6-A
Weapon System and IT System Programs
Analysis of Alternatives Development Procedures

1.1 Analysis of Alternatives Overview

While the use of analyses to support programmatic decisions is not new, the AoA process brings formality to the Concept Refinement phase by integrating the joint capabilities development and the pre-systems acquisition processes. In particular, the AoA process provides a forum for discussing risk, uncertainty, and the relative advantages and disadvantages of alternatives being considered to satisfy mission capabilities. The AoA shows the sensitivity of each alternative to possible changes in key assumptions (e.g., threat) or variable (e.g., performance capabilities) and represents one way for the MDA to address issues and questions early in pre-systems acquisition and during a program's life-cycle.

Involvement of senior experienced, and empowered individuals from both the Chief of Naval Operations (CNO)/Commandant of the Marine Corps (CMC) and the acquisition communities plays a key role in the analytical process. Periodic reviews prior to key decision points affords high-level visibility to potential programs, provides analytical rigor and flexibility for development of the initial acquisition strategy, and allows for coordination of effort between evolutionary increments and other defense programs. Review of in-progress analysis ensures the analysis addresses the key issues at hand and associated top-level architectural views, assumptions, and limitations.

1.2 Analysis of Alternatives Focus and Scope

The AoA supports milestone reviews and the development of follow-on Joint Capabilities Integration and Development System (JCIDS) documentation. Prior to commencement of any AoA study, it is necessary for programs to develop and receive approval on a Scope and Tasking Directive (i.e., an AoA Plan) at Concept Decision. The AoA Plan documents the incorporation of DoD and MDA guidance and allows senior leadership, in conjunction with the AoA IPT, to control the focus and scope of the AoA by adding to or deleting issues.

1. The scope of analysis should correlate to the amount of resources affected by the decision, with ACAT III programs receiving less analytical attention than ACAT I and II programs.

2. If the preferred alternative has already been identified by previous analyses and the MDA and CNO/CMC formally agree that all issues have already been resolved or that further analysis is unlikely to aid in the resolution of outstanding issues, a new analysis effort should not be initiated. (If these

conditions are met, the AoA may simply present the rationale and any existing analyses applicable to program decisions already made.)

3. For smaller programs, the analysis should be tailored and should be less rigorous than larger programs. However, in the unique situation where the resolution of substantive issues would benefit from a more rigorous process, the MDA should direct the conduct of a more in-depth analysis. Designation of independent activities to conduct the AoA for potential ACAT III and IV programs is encouraged, but not required.

4. AoAs for systems that are part of a SoS or FoS should include, within their scope, discussions on the interoperability requirements and concerns under which these system interoperate.

5. With few exceptions, technical studies are beyond the scope of an AoA. These studies are conducted under the supervision of the program manager who will then supply the results for incorporation in the AoA.

1.3 Initiation of the Analysis of Alternatives Process

The Program Sponsor, in coordination with the AoA IPT, will be responsible for developing the scope of analysis. At a minimum, this scope of analysis should identify the independent activity responsible for conducting the analysis, alternatives to be addressed, CNO (N81) approved campaign analysis model(s) to be used (when applicable), proposed completion date, operational constraints associated with the need, and specific issues to be addressed.

For potential SoS or FoS programs, the scope of the analysis should include at a minimum the SoS or FoS within which the program must interoperate. In addition, proponents should consider potential international participation as cooperative partners or as potential users of the systems.

Each issue should be well thought out to ensure the analysis is comprehensive and addresses the pertinent MDA-level issues to be resolved at the upcoming program decision point meeting.

1. The scope of the analysis is defined in a Scope and Tasking Directive (i.e., the AoA Plan) (see the next page after Table E6T1 for format) which is initially approved at Concept Decision at the start of the Concept Refinement phase by the individuals shown in the following table:

Table E6T1 AoA Scope of Analysis Approval Authorities		
ACAT ID	**ACAT IC, II, and III**	**ACAT IV**
ASN(RD&A), or designee, & CNO (N81) or CMC (DC, CD&I)	ASN(RD&A), or designee, & CNO (N81) or CMC (DC, CD&I)	MDA & CNO (N81) or CMC (DC, CD&I)

2. ASN(RD&A) or MDA, or designee, and CNO (N81) or CMC (DC,CD&I) will be jointly responsible for final scope of analysis approval. The Joint Analysis of Alternatives (AoA) Scope and Tasking Directive format is provided below.

JOINT ANALYSIS OF ALTERNATIVES (AoA)

SCOPE AND TASKING DIRECTIVE

SCOPE:

Program: [i.e. *Strike Directed Infra-Red Countermeasure (Strike DIRCM)*]

Proposed ACAT: [i.e. *II*]

Milestone: [i.e. *A*]

Analysis Director: [*Director's Name, Employer's Name or Agency*]

Executive Steering Committee (ESC):
[*List the principal decision makers here…*
USN: CNO (N8#) and DASN (AIR)
USMC: HQMC (ADC, A)]

AoA Integrated Product Team (IPT) Members:
[*List the members of the IPT, if established, here…*
USN: CNO (N1, N2, N3/5, N6, N81, N8#, N091),
PEO() (PMA-###-), *NSAWC*
USMC: APW, DC,CD&I, MAWTS-1
USAF: ACC – DRK, AF/XOR, SAF/AQPF]

Schedule
[i.e. *Analysis Plan Submitted to ESC*.....*01 Jan 08 (30 days)*
Analysis Plan Approved.....*01 Mar 08 (60 days)*
Interim Progress Review.....*30 Mar 08 (90 days)*
Interim Progress Review.....*01 May 08 (120 days)*
AoA Final Brief.....*30 May 08 (150 days)*
AoA Final Report.....*29 Jun 08 (180 days)*
Milestone A.....*4th Quarter, FY08*]

Background

Mission Need, Deficiencies and Opportunities. **[i.e. *Capability gaps to be addressed.*]**

Threats, Operational Environments, and Operational Concepts. [i.e. *What is the expected threat and what's the intelligence reference on which it is based? What is the expected operating environment, and what operational concepts are applicable?]*

Alternatives for consideration. [*Including existing programs and non-material solutions.*]

Alternative X. *Brief Explanation*

Alternative Y. *Brief Explanation…*

Scenarios: [Ex. *Scenarios will be based on the Strategic Planning Guidance (SPG) Defense Planning Scenarios. If required, excursions from scenarios will be approved by the ESC.*]

Models: [Ex. *The models used in the AoA will be selected by the Analysis Director and approved by the ESC. These will be selected based on their ability to address the issues identified in this tasking directive within the specified schedule. Where possible, commonly used and accredited DoD models, e.g., the Air Force Toolkit, will be used.*]

Purpose: [*Why is this AoA to be performed? What milestone is it in support of?*]

Measures of Effectiveness (MOE) and Key Issues: [i.e. *life-cycle cost, commonality, threats detected or countered, effectiveness, size/weight, availability/reliability, interoperability, situational awareness, level of maintenance, etc.*]

MOE 1. *Description and discussion.*

MOE 2. *Description and discussion…*

TASKING DIRECTIVE:

Guidance. [*Incorporate any D,PA&E guidance received if an ACAT 1 program. Ex. This AoA shall be conducted by the Analysis Director with the assistance of the AoA IPT per the above scope. The ESC shall approve the Analysis Plan, conduct the Formal Progress Reviews, and provide guidance to the Analysis Director to ensure that each service's equities and needs are adequately addressed. The Analysis Director shall be responsible for providing the AoA Final Report to the ESC and to the Milestone Decision Authority prior to Milestone A.*]

Constraints. [i.e. *limit analysis to specific platforms, limit study cost to $XX dollars, etc.*]

SUBMITTED:

Program Sponsor, Code	Date	PEO/SYSCOM/DRPM	Date

APPROVED:

CNO (N81) or CMC (DC,CD&I)	Date	ASN(RD&A), MDA or designee	Date

1.4 Oversight of the Analysis of Alternatives Process

1. When the scope of the AoA effort warrants, an AoA Integrated Product Team (IPT) consisting of appropriate members of the core ACT organizations, representatives from ASN(RD&A) Chief Systems Engineer (CHSENG), and other organization deemed appropriate by the MDA, will be assembled to assist the Analysis Director. The AoA IPT should be co-chaired by the cognizant PEO/SYSCOM/DRPM, or cognizant Deputy ASN(RD&A) if a PEO/SYSCOM/DRPM has not been assigned, and the Program Sponsor. When CNO/CMC requests, the AoA lead should be responsible for scheduling a formal briefing of the final results.

2. The purpose of the IPT is to oversee the AoA, provide advice and counsel to the independent analysis director, and make recommendations to ASN(RD&A) or the MDA and CNO/CMC. MDAs should ensure that an IPT is tailored in scope and size to each specific AoA. For potential programs that may be part of a SoS or FoS, the IPT should include representation from the SoS or FoS within which the program must be interoperable. The oversight provided by an IPT is intended to assess the validity and completeness of key program issues, alternatives, assumptions, Measures of Effectiveness (MOEs), integration and interoperability issues, international participation, process redesign approaches, scenarios, concept of operations and threat characteristics.

3. In the event consensus cannot be readily obtained at this oversight level, issues should be framed and raised for ASN(RD&A) or MDA and CNO (N8F)/CMC (DC,CD&I), or designee, resolution.

4. For Marine Corps programs, the AoA IPT is similarly composed with CMC (DC,P&R); CG, MCCDC; Marine Corps Systems Command (MARCORSYSCOM); and Marine Corps Operational Test and Evaluation Activity (MCOTEA) substituting for their Navy counterparts.

1.5 Analysis Director Role in the Process

An analysis director should be assigned by ASN(RD&A) for potential ACAT I and II programs or PEO/SYSCOM Commander/DRPM for potential ACAT III and IV programs to plan, lead, and coordinate funding for analysis efforts. Directors are independent of, but receive advice and counsel from an IPT.

1. Analysis directors should:

   a. Be independent of the PM.

   b. Have a strong background in analysis.

c. Have technical and operational credibility.

2. Once the AoA scope of analysis has been approved, the analysis director should draft the analysis plan. This plan should contain details associated with:

a. Issues to be addressed in the analysis.

b. Alternatives to be analyzed.

c. Scenarios (including the threat laydown) to be used.

d. Mathematical models or simulations to be employed.

e. MOEs (and as appropriate, associated Measures of Performance (MOPs)) to be used.

f. Work plan including a listing of responsibilities (effort and schedule) for supporting organizations.

g. Plan of action and milestones (POA&M) to support the program initiation schedule included in the approved scope of analysis.

3. Along with their other duties, analysis directors should:

a. Act as spokesperson by presenting periodic analysis briefings (see paragraph 1.9 on briefings/reports below).

b. Ensure that measures are taken to coordinate ACAT I program analysis efforts with all appropriate external agencies.

c. Organize an analysis team to assist in planning, conducting, and evaluating the analysis. This analysis team should include representatives from the organizations represented in the AoA IPT, as necessary.

4. In the event a contractor is employed as an analysis director, actions should be taken to avoid both the appearance and existence of a conflict of interest or potential future conflict of interest.

1.6 <u>CNO Role in the Analysis of Alternatives Process</u>

CNO (N8) will be jointly responsible with the ASN(RD&A) for top-level oversight of the AoA process. In this role, CNO (N8) will facilitate the process of arriving at consolidated CNO positions on matters relating to alternatives analysis and is the final CNO approval authority for ACAT I, II, and III program

analysis decisions. For ACAT IV programs, the Program Sponsor will perform these tasks.

1. CNO program sponsors will be responsible for providing active user representation on AoA IPTs, proposing an AoA scope of analysis, and planning and programming efforts. (PEOs/SYSCOMs or DRPMs/PMs, as appropriate, in conjunction with the cognizant resource sponsors, are responsible for budgeting for and execution of required funding to conduct AoAs.)

2. The Director of Naval Intelligence will validate the threat capability described in an AoA.

3. Director, Test and Evaluation and Technology Requirements (CNO (N091)) will provide advice and counsel with respect to MOEs and MOPs used in AoAs. The intent is to ensure that criteria used to justify acquisition decisions are either directly testable through MOEs or are indirectly testable through MOPs. CNO (N091) will forward MOEs and MOPs developed during the AoA to COMOPTEVFOR for review with respect to their testability.

4. Director, Assessment Division (CNO (N81)) is the CNO approval authority for AoA Scope and Tasking Directives and approval of all models and scenarios used in AoAs. CNO (N81) will be invited to join the AoA IPT.

5. CN0 (N8F) is the Executive Oversight Director of AoAs for warfare requirements. This does not relinquish the Program Sponsor’s AoA responsibilities, but ensures CNO (N8F)’s integration function is used to its fullest.

6. Director, Total Force Programming, Manpower, and Information Resources Management (CNO (N12)) is the point of contact for matters relating to manpower requirements analysis. The intent is to ensure IPTs fully explore manpower implications of new weapons systems and alternatives that favor reductions in manpower and personnel, and total life-cycle ownership cost.

7. Director of Naval Education and Training (CNO (N12)) is the point of contact for matters relating to individual training and education requirements analysis. The intent is to ensure IPTs fully explore individual training and education implications of new weapon systems and alternatives to optimize human performance and total system performance at minimum total life-cycle ownership costs.

1.7 CMC Role in the Analysis of Alternatives Process

CMC (DC,CD&I) is jointly responsible with the ASN(RD&A) for overseeing Marine Corps analysis activities. In this role, CMC (DC,CD&I) facilitates the process of arriving at consolidated

CMC positions on AoA matters and acts as the final CMC approval authority for AoA directors, analysis plans, and formal reports for ACAT I, II, III, and IV analyses.

1. In support of analyses that require Marine Corps-unique operations, CMC (DC,CD&I) will develop and accredit scenarios consistent with Defense Planning Guidance.

2. CMC (CG, MCCDC) will provide for active user representation to the analysis director, as well as planning, programming, budgeting, and execution funding for AoA activities conducted prior to program initiation.

3. As the resource allocator, CMC (DC,P&R) will plan, program, and budget funding to support AoA efforts following program initiation. In conjunction with PEOs/DRPMs/PMs, as appropriate, CMC (DC,P&R) will budget for these analysis efforts.

4. The Director of the United States Marine Corps Intelligence Activity (USMCIA) will validate the threat capability described in Marine Corps analyses.

5. MCOTEA personnel will provide advice and counsel with respect to MOEs and MOPs used in analyses. The intent is to ensure that criteria used to justify acquisition decisions are either directly testable through MOEs or are indirectly testable through MOPs. CMC (CG, MCCDC) will forward MOEs and MOPs developed during the AoA for Marine Corps programs to Director, MCOTEA for review with respect to their testability.

6. For ACAT I, II, III, and IV programs, the Marine Corps AoA Standing IPT provides advice and counsel to CMC (DC,CD&I). They review and prioritize analyses considering urgency of need, to ensure maximum efficiency in cost, time, and level of effort. The Standing IPT also advises the MDA on tailoring an AoA. During the conduct of formal analyses of alternatives, the IPT should provide guidance to the analysis director.

1.8 PM Role in the Analysis of Alternatives Process

As a member of the AoA IPT, the PM will provide the analysis director valuable advice and counsel, particularly regarding the executability of proposed alternatives, and technical issues such as manpower requirements, human performance and environmental, safety, and occupational health considerations, and training support. In conjunction with the resource sponsor, PMs will provide and execute analysis funding in support of the analysis director's plan. PMs will also be responsible for ensuring appropriate conflict of interest clauses are included in contracts for AoA-related services. The PM in coordination with a contracting officer will be responsible for providing feedback to industry so that AoA efforts can be coordinated with ongoing industrial concept refinement studies

which may be conducted under government contract. The intent is for both efforts to be comprehensive and complementary.

1.9 Briefings/Reports

1. Typically an AoA proceeds in the following five phases:

a. Planning.

b. Determination of performance drivers.

c. Determination of cost drivers.

d. Resolution of cost/performance issues.

e. Preparing final briefing and final report.

2. To ensure timely completion of the AoA to support program initiation, analysis directors will provide status briefings to the AoA IPT, ASN(RD&A), PEO/SYSCOM/DRPM, CNO (N8), and CMC (DC,CD&I), as requested.

3. At the end of the process, the AoA IPT reviews the final report and present a final briefing of results. The intent is to ensure all issues are addressed and that key finding are supported by the analysis. The AoA final results may be presented in the form of either a briefing and/or a formal report with approval as indicated in Table E6T2.

Table E6T2 AoA Final Report Approval Authorities

ACAT ID	ACAT IC, II, and III	ACAT IV
ASN(RD&A), or designee (flag or SES), & CNO (N8) or CMC (DC, CD&I)	MDA, or designee (flag or SES), & CNO (N8) or CMC (DC, CD&I)	MDA, or designee, & CNO Program Sponsor or CMC (DC, CD&I)

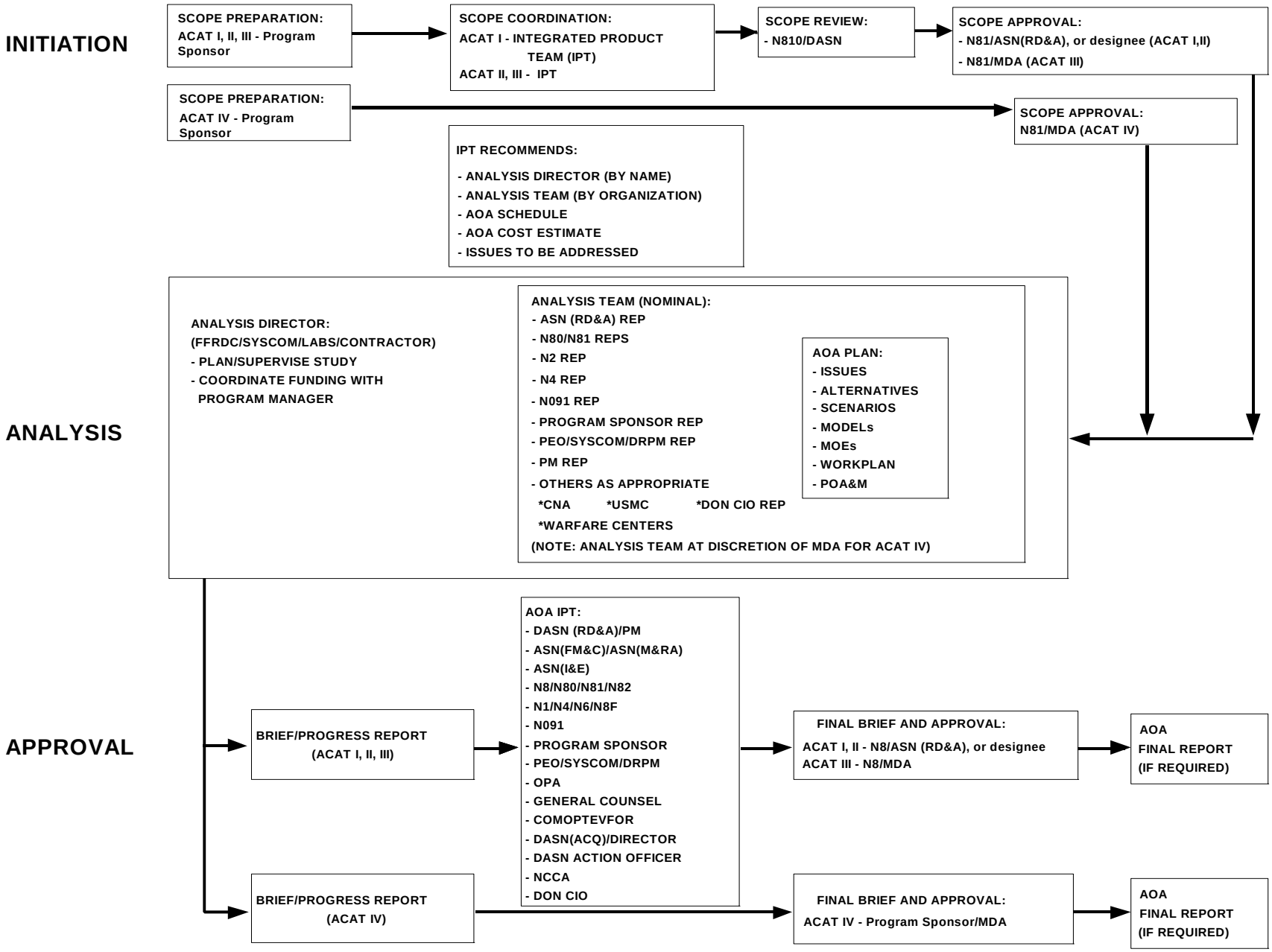
4. In the case of ACAT ID programs, ASN(RD&A) and CNO (N8) or CMC (DC,CD&I), as appropriate, approve the AoA performance parameters approximately 120 days prior to the Defense Acquisition Board (DAB), Defense Space Acquisition Board (DSAB), or Information Technology Acquisition Board (ITAB) date. This supports the follow-on development of the CDD/CPD/APB, as well as final Joint Requirements Oversight Council (JROC) approval and validation of the key performance parameters.

5. A copy of all ACAT I, II, III, and IV AoA final reports will be provided to ASN(RD&A) CHSENG, CNO (N81) or CMC (DC,CD&I), and COMOPTEVFOR, or Director, MCOTEA, as appropriate.

1.10 Navy Analysis of Alternatives Process

The Navy AoA process diagram is shown on the next page.

ASN(RD&A)/OPNAV AOA INITIATION, ANALYSIS, AND APPROVAL PROCESS



Chapter 7
Systems Engineering and Human Systems Integration

References:
(a) SECNAVINST 5000.2D
(b) OPNAVINST 3960.16A
(c) SECNAVINST 4855.3B
(d) SECNAVINST 4855.5 series
(e) MCO 4855.10B, Product Quality Deficiency Report (PQDR), of 26 Jan 93
(f) NAVSO P-3692, Independent Logistics Assessment Handbook, of Dec 03
(g) DOD Directive 5000.1, The Defense Acquisition System, of 12 May 03
(h) CJCSI 3170.01F, Joint Capabilities Integration and Development System, of 1 May 07
(i) SPAWARINST 5400.1A/NAVAIRINST 5400.158A/ NAVSEAINST 5400.97C/NAVSUPINST 5400.15/ NAVFACINST 5400.10, Virtual SYSCOM Engineering and Technical Authority Policy, of 31 Oct 06/31 Jan 07/27 Nov 06/12 Dec 06/7 Nov 06
(j) MARCORSYSCOM, C4I Integration and Interoperability Management Plan, of 2 Sep 05
(k) DOD Instruction 8510.01, Defense Information Assurance Certification and Accreditation Process (DIACAP), of 28 Nov 07
(l) MIL-HDBK-237D, Electromagnetic Environmental Effects and Spectrum Certification Guidance for the Acquisition Process, of 20 May 05
(m) SECNAVINST 5200.39A
(n) OPNAVINST 1001.21B
(o) USD(P&R) memorandum, Interim Policy and Procedures for Strategic Manpower Planning and Development of Manpower Estimates, of 10 Dec 03
(p) OPNAVINST 1500.76A
(q) DOD Instruction 5000.02, Operation of the Defense Acquisition System, of 8 Dec 08
(r) Assistant Secretary of the Navy (Installations and Environment) Memorandum 99-01, Requirements for Environmental Considerations in Test Site Selection, of 11 May 99
(s) OPNAVINST 5100.23G
(t) SECNAVINST 5100.10J
(u) OPNAVINST 5090.1C
(v) DOD Instruction 4160.21-M-1, Defense Demilitarization Manual, of 21 Oct 91
(w) DOD Instruction 4160.21-M, Defense Materiel Disposition Manual, of 18 Aug 97
(x) NAVSEA OP 4, Ammunition and Explosives Safety Afloat, of 15 Jan 03
(y) OPNAVINST 8020.14/MCO P8020.11
(z) SECNAVINST 4140.2
(aa) DOD 4140.1-R, DoD Supply Chain Materiel Management Regulation, of 23 May 03

(ab) Public Law 108-136, National Defense Authorization Act for Fiscal Year 2004, Section 802, Quality Control In Procurement Of Aviation Critical Safety Items And Related Services, of 24 Nov 03

7.1 Systems Engineering

Program managers (PMs) shall define and implement a disciplined approach for assuring and measuring the quality and reliability of systems during development and production per reference (a).

A systems engineering plan (SEP) is the means for a disciplined approach for planning and managing the systems engineering effort. The SEP shall address the overall systems engineering process to be used, how this process relates to the overall program, how the technical baseline will be managed, and how technical reviews will be used as a means to ascertaining program technical risk per reference (a).

Per reference (a), all programs responding to a capabilities or requirements document, regardless of acquisition category, shall apply a robust systems engineering approach that balances total system performance and total ownership costs within the family of systems (FoS), systems of systems (SoS) context. Programs shall develop a SEP for milestone decision authority (MDA) approval, in conjunction with each milestone review, and integrated with the acquisition strategy (see paragraph 3.9.1). This plan should describe the program's overall technical approach, including processes, resources, metrics, and applicable performance incentives. It should also detail the timing, conduct, and success criteria of technical reviews. SEPs are submitted by the Direct Reporting Program Manager (DRPM)/PM and program lead or chief systems engineer; concurred with by the Program Executive Officer (PEO) or equivalent, PEO/Systems Command (SYSCOM) lead or chief systems engineer, and Office of the Under Secretary of Defense (Acquisition, Technology and Logistics) (OUSD(AT&L)) Deputy Director Defense Systems systems engineer (for acquisition category (ACAT) ID/IAM programs); approved at the Component-level by the Component Acquisition Executive (Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN(RD&A)) (for ACAT ID and IAM programs); approved by the MDA. See Annex 7-A for the signature cover pages associated with the appropriate ACAT level program. See ASN(RD&A) memorandum of 16 Nov 07 for SEP development, review, and approval guidance.

Hazards and risk assessments, including environmental, safety, and health considerations, should be conducted to identify and mitigate factors that could impact the development, production, operation, and sustainment of the system with respect to total system cost, schedule, and performance. PMs should

provide for independent developing activity (DA) technical review and independent DA technical risk assessment of programs. Formal systems engineering technical reviews should be used as the means for continuous assessment of program technical health. These reviews, when conducted by the program team together with independent DA subject matter experts at appropriate event-based points in a program, can be an effective approach to managing the technical baseline (performance requirements, design trade-offs, certification and validation requirements, development and production costs, and schedule as an integrated whole), technical risk, and overall program technical health.

See the Defense Acquisition Guidebook for implementation guidance for all Department of the Navy (DON) programs.

7.1.1 Manufacturing and Production

Manufacturing and production activities are those activities associated with the concurrent development and maturation of the product design for production, manufacturing, and the establishment of the required production and post-production resources and capabilities. It also includes transition-to-production planning to smoothly move from the design/development phase into low- and high-rate production with minimal risks. This planning should ensure:

1. The details of the design and production planning process are integrated into the program plan and master schedule,

2. Key product characteristics, critical safety items, and critical application items are identified during the design phase,

3. Design for producibility, manufacture and assembly is performed. Design trade studies should be accomplished to ensure product designs that are tolerant to variation expected in the intended manufacturing, assembly, test, and usage environments,

4. Key manufacturing process characteristics are identified and the associated manufacturing processes requirements are defined and developed concurrent with product design. Variability reduction planning should identify the approach toward implementing process controls on key system design characteristics,

5. Hard tooling, test equipment, and calibration/metrology/ measurement system is validated for low rate and full rate production,

6. Manufacturing processes are proofed/validated

7. Effectiveness of Manufacturing Resource Planning/ Enterprise Resource Planning,

8. Identification of production capacity and bottlenecks with work-arounds,

9. Diminishing manufacturing sources/parts obsolescence planning,

10. Discrepancy root cause and corrective action system implementation,

11. Management of subcontractors/suppliers, and special processing facilities (e.g., heat treatment, etc), and

12. Production readiness reviews conducted to assess readiness of the baselined product and the associated manufacturing resources/processes to begin low- and/or high-rate production.

7.1.1.1 Test, Measurement, and Diagnostic System Support

PMs should establish metrology and calibration (METCAL) requirements early in the acquisition cycle to assure that measurements and related test and calibration decision risks are commensurate with the needs of each phase of an acquisition program. These requirements are per reference (b) and include the following:

7.1.1.1.1 Measurement Traceability and Compatibility

Measurements should be traceable through national standards maintained by the National Institute of Standards and Technology (NIST) to the International System of Units (SI) of measurements, or to natural constants whose values in terms of the SI units are known and recommended by the General Conference of Weights and Measures, and compatible within the affected contractor and defense organizations, and applicable allied nations.

7.1.1.1.2 Measurement Technology

Measurement technology should be available, suitable, and effective to support test, measurement, and calibration requirements of all phases of an acquisition. New or improved measurement technology required by an acquisition program should be developed concurrently with the program.

7.1.2 Quality

The quality program should ensure the use of best engineering, design, manufacturing and management practices that emphasize the prevention of defects. Quality should be designed into the product through the systems engineering design process to define the product and process quality requirements. Contractors should propose a quality management process that meets required program support capabilities. The quality

management system may be based on the fundamentals described in the ISO-9001 series supplemented by AS9100, International Aerospace Quality Standard, which provide a basic minimum quality system model. Additional advanced quality requirements should be considered for systems based on factors such as risk, design complexity, and maturity, process complexity and maturity, safety, and economics. An advanced quality system builds on a basic quality system, especially during the design/development phase, by identifying critical product and process characteristics, design-to-manufacturing process capabilities, design for assembly and manufacturing, design to control process variability, process controls, continuous improvements, etc. The quality management approach should include an assessment of the contractor's quality management process and its implementation, including those related to assessments or oversight of subcontractors, suppliers, and special process facilities (e.g., heat treatment). The quality system should provide timely notification and feedback to contracting and program offices in areas such as major and critical deficiencies, potential manufacturing process problems, and subcontractor, supplier, or special process facilities problems that potentially impact the program.

7.1.2.1 <u>Past Performance</u>

Reference (c) provides specific procedures for obtaining past performance quality information, using the Product Data Reporting and Evaluation Program.

7.1.2.2 <u>Deficiency Reporting</u>

PMs should report discrepancies or deficiencies in material shipments and request billing adjustments (see 41 CFR 101) and implement corrective/preventative actions to preclude recurrence of quality deficiencies.

Reference (c) provides policies, procedures and responsibilities for implementing and monitoring a unified, automated product data reporting and evaluation system.

Reference (d) provides procedures for reporting product deficiencies across component lines.

Reference (e) provides specific Marine Corps product quality deficiency reporting procedures.

7.1.3 Acquisition Logistics and Sustainment

Reference (f) provides the PM with a framework and road map for structuring and executing successful logistics support programs throughout the system life cycle.

7.1.3.1 Life Cycle Logistics (LCL)

LCL includes the logistics functions from the acquisition phase through the sustainment phase. LCL means that major program decisions are assessed, weighed, and justified in terms of that decision's effect on resultant system or increment operational effectiveness, long-term sustained material readiness, and the affordability to operate and maintain across the expected life cycle.

7.1.3.2 Total Life Cycle Systems Management (TLCSM)

Per reference (g), TLCSM is the implementation, management, and oversight of all activities associated with the acquisition, development, production, fielding, sustainment, and disposal of a defense system across its life cycle. TLCSM bases major system development decisions on their effect on life cycle operational effectiveness and logistics affordability. The TLCSM decision model encompasses, but is not limited to, the following:

1. Evolutionary acquisition strategies, including support,

2. Supportability performance criteria, as defined in reference (h) under "operational effectiveness",

3. Cost-related performance and metrics (some variant of cost-per-operating-period),

4. Performance-based logistics strategies and associated metrics,

5. Increased reliability and reduced logistics footprint, and

6. Continuous review and revision of sustainment strategies.

Implementation of the TLCSM business approach; by capabilities development, and program and contracting management; means that all major materiel alternative considerations and all major acquisition functional decisions demonstrate an understanding of the effects, during consequential operations and sustainment phase, of system effectiveness and affordability.

7.1.3.3 Program Manager's LCL Responsibility

Per reference (g), PMs establish innovative logistics support and sustainment programs, using best practice and technology solutions. The choice of logistics support strategy is based and presented on well-documented analyses that system operational effectiveness and life cycle affordability can be satisfied using Department of Defense (DoD)'s and private industry's operational and logistics infrastructure. Decisions are updated to satisfy iterative changes in formal criteria; with the result that system performance is interoperable and meets Joint Capabilities Integration and Development System (JCIDS) and JCIDS-related performance capabilities criteria.

7.1.3.4 Warfighter Supportability-Related Performance

Understanding warfighter needs for short and long-term sustained material readiness, sustained operational effectiveness and availability, and continued operational affordability is essential to any logistics support strategy. PMs must transcribe changed performance specifications into the logistics support strategy and program, as situations change and as the operational environment evolves. For example: PMs needing to invest in technological upgrades for embedded diagnostics should rely for investment justification on formally specified warfighter criteria for high reliability and built-in-test performance.

7.1.3.5 Supportability

Effective sustainment of weapons systems (including minimal "logistics footprint") begins with the design, development, and/or procurement of reliable, maintainable, and diagnostically effective systems. This is achieved in part through a robust systems engineering methodology that focuses on total system/total life-cycle performance. Supportability and cost-related specifications are an integral part of the systems engineering process.

7.1.3.6 Supportability Analyses

Supportability analyses are a key part of the overall acquisition strategy, source selection, and system design and should be accomplished in support of these activities throughout the acquisition process.

Supportability analyses should support acquisition planning, level of repair and reliability-centered maintenance decisions, program tradeoffs, and the formation of contract provisions.

See the Defense Acquisition Guidebook for implementation guidance for all DON programs.

7.1.3.7 Support Concepts

Support concepts, including Performance Based Logistics (PBL) and the associated business case analysis discussed in paragraph 3.4.7, should satisfy user's CDD/CPD-specified requirements for sustaining support performance at the lowest possible life-cycle cost. To this end, acquisition planning documents should document, for each evolutionary increment of capability to be delivered, the plans, resources, and metrics that will be used to execute and measure these five mandatory logistics support concepts:

1. Minimal total life-cycle cost to own and operate (i.e., minimal total ownership cost),

2. Maintenance concepts that optimize both organic and industry sources,

3. Availability of support to meet warfighter-specified levels of war and peacetime performance, and

4. Logistics support that sustains and continuously improves both short and long-term material readiness.

5. Training concepts that describe the training to met short and long-term sustained material readiness

See the Defense Acquisition Guidebook for implementation guidance for all DON programs.

7.1.3.8 Support Data

The DON's database for the dissemination of weapon system operating and support (O&S) costs is the DON Visibility and Management of Operating and Support Costs (VAMOSC). Naval Center for Cost Analysis (NCCA) should have overall program management responsibility for VAMOSC. See the Defense Acquisition Guidebook for implementation guidance for all DON programs.

7.1.3.8.1 Sources for Support Related Data

Obtain supportability-related program data through the use of Logistics Management Information (LMI) summaries. Refer to MIL-PRF-49506, Logistics Management Information, and MIL-HDBK-502, DOD Handbook - Acquisition Logistics, for guidance.

7.1.3.9 Support Resources

Support analyses should determine integrated logistics support resource requirements for the program's initial planning, execution, and life-cycle support. Recommendations for entry into subsequent phases should be based on adequate support resources being budgeted to meet and sustain support performance threshold values. Planning, Programming, Budgeting, and

Execution System (PPBES) budget item documentation or the Logistics Requirements and Funding Summary Annex of the discretionary Supportability Plan, will show whether or not adequate funding has been budgeted to fully support the end item. See the Defense Acquisition Guidebook for implementation guidance for all DON programs.

7.1.4 Open Architecture

See reference (a) for guidance and direction.

Naval open architecture is an extension and Navy implementation of the USD(AT&L)'s Modular Open Systems Approach. Naval open architecture should be applied as an integrated technical approach and used for all systems, including support systems. Naval open architecture principles include:

Modular design and design disclosure to permit evolutionary design, technology insertion, competitive innovation, and alternative competitive approaches from multiple qualified sources.

Reusable application software derived from best value candidates reviewed by subject matter expert peers and selected based on data-driven analyses and experimentation. Design disclosure and source code should be made available for evolutionary improvement to all qualified sources.

Interoperable joint warfighting applications and secure information exchange using common services (e.g., common time reference), common warfighting applications (e.g., open architecture track manager) and information assurance as intrinsic design elements.

Life-cycle affordability which includes system design, development, delivery, and support. Concurrently mitigating ongoing Commercial-Off-The-Shelf (COTS) obsolescence by exploiting the Rapid Capability Insertion Process/Advanced Processor Build (RCIP/APB) methodology for sustained performance enhancement.

Encouraging competition and collaboration through development of alternative solutions and sources.

7.1.5 Reliability, Availability, and Maintainability (RAM)

As part of the performance requirements, a design reference mission profile should be developed that includes functional and environmental profiles.

Parts derating criteria should be mutually agreed upon between the contractor and the government and must consider past component history, environmental stresses, and component criticality under worst-case mission profile environments.

Accelerated test methods (e.g., step stress testing, accelerated life testing, and reliability growth testing) should be used to assure design maturity prior to operational testing.

Provisions for failure data collection, reporting, and analyses should be established and mutually agreed upon between the government and the contractor.

Built-In-Test, testability, and false alarm requirements should be defined and a plan to achieve requirements maturity implemented. A guide titled "Technical Brief on Built-In-Test, Design and Optimization Guidelines (October 2001)" is available on the DASN(RD&A)ALM Acquisition One Source web page at http://acquisition.navy.mil/content/view/full/825.

See the Defense Acquisition Guidebook for implementation guidance for all DON programs.

7.1.6 Interoperability and Integration

See reference (a) for guidance and direction.

[***fm SNI 5000.2D, 7.1.6, second subparagraph: During the Concept Refinement Phase and the Technology Development Phases, interoperability shall be addressed by including SoS or FoS considerations in applicable analyses. If Technology Development activity is carried out, the PM shall ensure that the technologies developed will have no adverse affect on interoperability and integration at the SoS or FoS level. During the System Development and Demonstration phase, the PM shall ensure that interoperability is being maintained.***] PMs should plan to participate as data producers or data consumers in Community of Interest (COI) pilots for technical risk reduction efforts for the programs involved.

7.1.6.1 IT Design Considerations

See reference (a) for guidance and direction.

7.1.6.2 DoD Architecture Framework/Defense Information Technology Standards Registry (DISR)

DoD Joint Technical Architecture (JTA) has been replaced by the DISR. See reference (a) for guidance and direction.

7.1.6.2.1 Transformational Communications Architecture (TCA)

TCA is essentially a network of interconnected capabilities that span the DoD, National Aeronautics and Space Administration (NASA), and the Intelligence communities and that enable independent and interoperable connectivity through the

coordinated mandate of standards, jointly controlled interfaces, and protocols.

An executive summary of the Transformational Communications Architecture (TCA) Baseline Version 2.0 will be available as a reference link in an updated version of the FORCEnet Consolidated Compliance Checklist (FCCC). The TCA Baseline Version 2.0 document represents the culmination of over eighteen months of work focused on evolving the TCA from a concept into a series of executable programs that will connect the DoD, NASA, and the Intelligence communities. The TCA Baseline Version 2.0 document provides a technical foundation for enabling and guiding development of U.S. Government communications capabilities for the next two decades.

7.1.6.2.2 Joint Tactical Radio System (JTRS) Software Compliant Architecture (SCA)

The JTRS will provide critical communications capabilities for the tactical wireless tails of the Global Information Grid (GIG). JTRS and SCA continue to evolve and have become a cornerstone to provide future net-centric capabilities to the warfighters. All communications waveforms/systems that operate at or above 2 Gigahertz (GHz) are required to be developed in compliance with JTRS SCA. All JTRS/SCA radios should be able to run the networking services layer of the wideband networking waveform (WNW), support internet packed routing on the user and network sides of the radio, and should incorporate National Security Agency (NSA) certified software programmable cryptology.

7.1.6.2.3 Teleports

DoD Teleports will provide the warfighter net-centric internet protocol (IP) access to the Global Information Grid (GIG). The DoD Teleport architecture is an environment that provides deployed forces with sufficient interfaces for multi-band and multi-media connectivity from worldwide locations to Defense Information System Network (DISN) Service Delivery Nodes (SDN) and tactical command, control, communications, computers, and intelligence (C4I) systems. This system will facilitate the interoperability between multiple Satellite Communications (SATCOM) systems and deployed tactical networks, thus providing the user a seamless interface into the DISN and C4I systems.

7.1.6.2.4 Joint Battle Management Command and Control (JBMC2)

The JBMC2 roadmap defines the long-range goals for JBMC2 and the Joint and Services' programs that support those goals. JBMC2 is a construct that consists of the processes, architectures, systems, standards, and command and control operational concepts employed by the Joint Force Commander during the planning, coordination, directing, controlling, and assessing of Joint force operations from interface with strategic level

through the tactical level. A reference link to the JBMC2 roadmap will be available in an updated version of the FCCC.

7.1.6.3 FORCEnet Integrated Architecture

Joint/multinational interoperability and information assurance are key elements of the FCCC. They will be addressed through adherence to Department of Defense (DoD) approved standards and participation in DoD certification processes.

FORCEnet capabilities are described by the FORCEnet Functional Concept of 7 Feb 05. Additional information, including source documents, may be obtained from CNO (N6/N7) FRCC memorandum of 27 May 05.

7.1.6.3.1 System of Systems (SoS) or Family of Systems (FoS) Integration and Interoperability Validation

7.1.6.3.2 FORCEnet Integrated Management Plan

An integrated Navy/Marine Corps FORCEnet integration and interoperability management plan is being developed jointly by COMSPAWARSYSCOM (FORCEnet CHENG) and MARCORSYSCOM in coordination with ASN(RD&A) CHSENG to refine and integrate the tools and processes for program assessment and data management and address configuration management and execution phase governance. The plan will define the process for SoS or FoS engineering and interoperability validation.

ASN(RD&A) CHSENG will work with DON Chief Information Officer (CIO), Deputy DON CIO (Navy), PEO(EIS), and Naval Network Warfare Command (NETWARCOM) to incorporate the business domain into the FORCEnet integrated architecture and to integrate business and warfighting IT acquisition processes and databases.

7.1.6.3.3 FORCEnet Efficiency and Effectiveness

FORCEnet implementation will require efficient and effective processes and practices. Unnecessarily redundant processes and practices should be eliminated. FORCEnet implementation should use existing processes wherever feasible and should employ efficient information management strategies and practices, including the "enter once use often" strategy for databases. Implementation managers should take advantage of the ASN(RD&A) CHSENG Naval Collaborative Engineering Environment, which offers common processes, practices, procedures, databases, and products.

7.1.6.3.4 Roles and Responsibilities for FORCEnet Implementation Within the Acquisition Community

Commander, Naval Network Warfare Command (NETWARCOM) and Commanding General, Marine Corps Combat Development Command (MCCDC) have the lead in developing the operational views (OVs). ASN(RD&A) Chief Systems Engineer (CHSENG) will oversee development of FORCEnet integrated architecture system views and technical views (SVs and TVs) through the architecture governance process. The responsibilities of the COMSPAWARSYSCOM (FORCEnet CHENG) and other members of the DON acquisition community for developing system views (SVs) and technical views (TVs) are included in the below roles and responsibility statements per ASN(RD&A) memorandum of 14 Jul 05.

1. Assistant Secretary of the Navy, Research, Development, and Acquisition (ASN(RD&A))

a. Provides overall guidance and direction for the Department of the Navy (DON) acquisition community's participation in the FORCEnet implementation process.

b. Resolves system integration issues that cannot be resolved at a lower level.

c. As Component Acquisition Executive, ensures compliance with FORCEnet policies, architecture, and standards during program reviews and milestone decisions.

d. Coordinates with the Chief of Naval Operations (OPNAV) and Headquarters Marine Corps (HQMC) resource and warfare sponsors to address any cost, performance, or schedule impacts associated with modifying legacy systems to comply with FORCEnet standards.

e. Coordinates with OPNAV and HQMC to identify funding for FORCEnet implementation.

f. Coordinates with Department of the Navy (DON) Chief Information Officer (CIO) to ensure compliance with DON information management and information technology (IT) policies.

g. Coordinates with OPNAV, MCCDC, and Fleet Forces Command N6/NETWARCOM to designate legacy programs as FORCEnet programs.

2. Assistant Secretary of the Navy, Research, Development, and Acquisition, Chief Systems Engineer (ASN(RD&A) CHSENG)

a. Oversees the development of the FORCEnet integrated architecture SVs and TVs through the architecture governance process.

b. Advises ASN(RD&A) on the resolution of cross-systems command (SYSCOM) integration issues.

c. In coordination with appropriate Deputy Assistant Secretaries of the Navy (DASNs), facilitates resolution of cross-service and cross-agency technical interoperability issues with counterpart service and agency acquisition executives.

d. Facilitates development of a FORCEnet integration and interoperability management plan. Ensures coordination of the plan with related initiatives, including the Program Executive Officer for Integrated Warfare Systems (PEO (IWS))-led Open Architecture initiative and the PEO for Command, Control, Communications, Computers, Intelligence and Space (PEO (C4I and Space))-led Net-Centric Enterprise Solutions for Interoperability (NESI) initiative.

e. Coordinates and oversees the implementation of this policy, and makes revision recommendations to ASN(RD&A).

f. Provides Naval representatives to the Department of Defense (DoD) IT Standards Registry (DISR) IT Standards Working Groups to ensure that both mandated and emerging FORCEnet and joint standards are included in DISRonline.

3. Commander, Space and Naval Warfare Systems Command (COMSPAWARSYSCOM) (FORCEnet/Command, Control, Communications, Computers, Intelligence (C4I) Chief Engineer (CHENG))

a. Provides overall technical guidance and advice for implementing FORCEnet.

b. Leads the development of the enterprise-wide FORCEnet integrated architecture SVs and TVs in coordination with MARCORSYSCOM, and ensures integration with the NETWARCOM and MCCDC-developed OVs. Provides guidance and support to programs in their development of program specific SVs and TVs and ensures they are consistent with the overarching views. Works with PEO (IWS) and the Open Architecture Enterprise Team (OAET) to coordinate FORCEnet architecture development and Naval Open Architecture efforts. When directed, coordinates with the ASN(RD&A) CHSENG, Program Executive Officer for Information Technology (PEO (IT)), Direct Reporting Program Manager (DRPM) NMCI, DON CIO, and Deputy DON CIO (Navy) for integration of business IT architecture and standards with the FORCEnet integrated architecture and standards.

c. In collaboration with ASN(RD&A) CHSENG, Marine Corps Systems Command (MARCORSYSCOM), and other stakeholders, develops and manages the FORCEnet compliance process and associated processes, ensuring efficiency, effectiveness, and minimal additional workload on program managers.

d. Leads the FORCEnet/C4I Virtual SYSCOM, and coordinates efforts with the other Virtual SYSCOMs.

e. Participates with MARCORSYSCOM under ASN(RD&A) CHSENG oversight in the development of a FORCEnet integration and interoperability management plan.

f. Leads the integration and interoperability validation of FORCEnet FoS.

g. Coordinates acquisition community participation in FORCEnet experimentation with other acquisition community participants, NETWARCOM, and MCCDC.

h. Collaborates with NETWARCOM and other stakeholders to ensure that the FORCEnet integrated architecture is properly integrated with the GIG integrated architecture and approved multinational information sharing architectures.

i. Leads FORCEnet industry outreach and participation in industry standards forums.

j. Serves as FORCEnet Technical Authority (TA) per reference (i).

k. Guides, supports, and oversees FORCEnet testing and certification of individual systems as compliant with applicable FORCEnet technical standards.

l. Coordinates development of common data reference models per the DoD Data Management Strategy.

4. Commander, Space and Naval Warfare Systems Command (COMSPAWARSYSCOM) (roles and responsibilities as SYSCOM commander in addition to COMSPAWARSYSCOM (FORCEnet CHENG) roles and responsibilities defined above)

a. Guides, supports, and oversees FORCEnet implementation in SPAWARSYSCOM systems.

b. Participates in integration and interoperability validation of FORCEnet FoS involving SPAWARSYSCOM systems.

c. Provides FORCEnet integration and interoperability support for SPAWARSYSCOM systems.

5. Commander, Naval Air Systems Command (COMNAVAIRSYSCOM)

a. Per COMSPAWARSYSCOM (FORCEnet CHENG) guidance, supports and oversees FORCEnet implementation in NAVAIRSYSCOM systems.

b. Participates in the development of the FORCEnet integrated architecture SVs and TVs to ensure appropriate representation of NAVAIRSYSCOM systems and Sea Strike capabilities.

c. Supports integration and interoperability validation of FORCEnet FoS involving NAVAIRSYSCOM systems.

d. Provides FORCEnet integration and interoperability support for NAVAIRSYSCOM systems.

6. Commander, Naval Sea Systems Command (COMNAVSEASYSCOM)

a. Per COMSPAWARSYSCOM (FORCEnet CHENG) guidance, supports and oversees FORCEnet implementation in NAVSEASYSCOM systems.

b. Participates in the development of the FORCEnet integrated architecture SVs and TVs to ensure appropriate representation of NAVSEASYSCOM systems and Sea Shield and Sea Basing capabilities.

c. Supports integration and interoperability validation of FORCEnet FoS involving NAVSEASYSCOM systems.

d. Provides FORCEnet integration and interoperability support for NAVSEASYSCOM systems.

7. Commanding General, Marine Corps Systems Command (CG, MARCORSYSCOM)

a. Per COMSPAWARSYSCOM (FORCEnet CHENG) guidance, supports and oversees FORCEnet implementation in MARCORSYSCOM systems.

b. Participates in the development of the FORCEnet integrated architecture SVs and TVs to ensure appropriate representation of MARCORSYSCOM systems and Expeditionary Warfare and Sea Basing capabilities.

c. Supports integration and interoperability validation of FORCEnet SoS or FoS involving MARCORSYSCOM systems.

d. Through the Deputy Commander for C4I Integration, ensures that reference (j) is aligned with the FORCEnet management process; collaborates with COMSPAWARSYSCOM (FORCEnet CHENG) under ASN(RD&A) CHSENG oversight to develop a FORCEnet integration and interoperability management plan.

e. Provides FORCEnet integration and interoperability support for MARCORSYSCOM systems.

8. Program Deputy Assistant Secretaries of the Navy (DASNs)

a. Oversee FORCEnet compliance of programs under their purview, and advise ASN(RD&A) on the resolution of architecture, standards, and system integration issues.

9. Program Executive Officers (PEOs), Direct Reporting Program Managers (DRPMs), and Program Managers (PMs) of FORCEnet Programs

a. Bring programs into compliance with funded FORCEnet requirements, as defined in revised capability documents, and with the applicable FORCEnet technical standards and System Performance Documents (SPDs).

b. Provide and update data to the databases and toolsets approved by the COMSPAWARSYSCOM (FORCEnet CHENG) and participate in program assessments.

c. Develop program specific SVs and TVs and ensure they are consistent with the overarching FORCEnet views in the Integrated Architecture.

d. Address FORCEnet compliance in program cost estimates and within the Planning, Programming, Budgeting, and Execution (PPBE) process; work with the program and resource sponsors and the COMSPAWARSYSCOM (FORCEnet CHENG) to agree on the applicable FORCEnet capabilities and technical standards in consideration of available funding and effect on program cost, performance, and schedule of any system modifications required.

e. Participate in the integration and interoperability validation of FORCEnet FoS under their purview, including participation in System Engineering Integrated Product Team (SE IPTs) and development of applicable SPDs.

f. Consistent with program and resource sponsor guidance and the Navy Comptroller rules for proper use of various appropriations, use system capability improvement and maintenance funding as an opportunity to enhance compliance with FORCEnet technical standards.

g. Report the status of FORCEnet compliance at each milestone and program review.

h. Comply with the information security certification requirements of reference (k).

10. Program Executive Officer for Integrated Warfare Systems (PEO (IWS))

a. Coordinates Naval Open Architecture efforts with FORCEnet implementation.

11. DON Milestone Decision Authorities (MDAs)

a. Ensure compliance with FORCEnet policies and integrated architecture during program reviews and milestone decisions.

7.1.6.4 Interoperability and Integration Support

Per reference (a), system design shall take into account potential international program ramifications as an integral part of the design process. For international cooperative programs, these design considerations are mandatory. For U.S.-only development efforts, the PM shall consider designing the proposed system with a potential for eventual international sales and support.

7.1.7 Survivability

See reference (a) for guidance and direction.

7.1.8 Shipboard Systems Integration

A ship System Design Specification will include interface definitions and interoperability characteristics. Integrated topside design, which is part of the ship systems engineering process, is a key activity for maintaining battle force interoperability and mission effectiveness. A systems engineering process, which balances the competing requirements posed by combat capability, ship signatures, global connectivity, and quality-of-life solutions must be applied to ship design. The intent of establishing a ship System Design Specification within the context of the total ship is to deliver safe and effective topsides. The drivers include:

1. Operability: Ensure that sufficient total ship integration has occurred to provide confidence in the basic performance of the ship and its systems.

2. Interoperability: Ensure that sufficient cross-platform integration has occurred to provide confidence in satisfactory operation of the ship within a joint battle force.

3. Safety and Survivability: Ensure that sufficient engineering rigor and total shipboard systems integration have been applied to provide confidence in the safety and survivability of the ship and its personnel.

Ship PMs should facilitate an integrated topside design approach in both ship design and system development. Exercise discipline in technology insertion and deployment on new systems into ships' topsides per reference (a).

Ship PMs shall facilitate lower total ownership cost (TOC) for new and legacy ships per reference (a). Economic advantages allow pursuit of:

1. Cost Avoidance: Comprehensive topside pre-planned product improvement (P3I) strategies enable lowered costs of ship upgrades and less rework cost. Improved practices, materials, and standards (e.g., corrosion control, new technology) enable less maintenance workload.

2. Smaller Fleet Inventory: A constrained number of topside systems, shared apertures and common architecture enable a smaller overall piece-part set as well as a consolidated training approach.

7.1.9 Performance Specifications

See reference (a) for guidance and direction.

7.1.9.1 System Performance for SoS and FoS Programs

The SPD shall serve as the basis for PMs to develop or modify individual systems specifications under their cognizance per reference (a). A SoS or FoS SPD shall be jointly approved by the respective PMs per reference (a). After Milestone B, or Milestone C if program initiation, ASN(RD&A) will use the SPD as a means for maintaining alignment between programs during execution of the acquisition process.

SoS/FoS and net-centric considerations are:

1. Competencies needed for the job/task, ensuring the skills and knowledge requirements are within the human capability domain minimizing problems in training and operation.

2. Designing systems with summary and drill-down functionality, providing users at various levels of access information critical to their assigned jobs e.g. individual and group situational awareness.

3. Complexities in a knowledge mapping approach – developing an adaptive system for the warfighter with an understanding of what each needs to know to perform the job/task, with customized individual or group information access and representation.

4. Individual and group integrated web-based tools. Authoring, formatting, decision-making tools for individuals and groups that facilitate information dissemination and absorption

that will be critical to ensure the Warfighter is not overwhelmed with the information and publishing process itself.

7.1.9.2 Standardization and Commonality

See reference (a) for guidance and direction.

7.1.10 Precise Time and Time Interval (PTTI) Support

To ensure uniformity in precise time and time interval operations, Coordinated Universal Time (UTC), traceable to UTC(USNO) maintained by the United States Naval Observatory (USNO), is mandated for the time of day information exchanged among DoD systems. Traceability to UTC(USNO) may be achieved by various means depending on system specific accuracy requirements.

7.1.11 Geospatial Information and Services (GI&S)

See reference (a) for guidance and support.

7.1.12 Natural Environmental Support

See reference (a) for guidance and support.

7.1.13 Electromagnetic Environmental Effects (E3) and Spectrum Supportability

E3 on equipment, systems, or platforms are critical elements that must be considered throughout the acquisition process to ensure the successful operational effectiveness of these military assets in support of the warfighter. Reference (l) contains detailed information on all the processes and documents used by the Spectrum Management and E3 communities and should be consulted for additional information.

7.1.14 Integrated Product and Process Development (IPPD)

PEOs, SYSCOM Commanders, DRPMs, and PMs should ensure the elements of IPPD are implemented in executing all programs under their cognizance. See the Defense Acquisition Guidebook for implementation guidance for all DON ACAT programs.

7.1.14.1 Integrated Product Teams (IPTs) and IPPD

For systems being designed for ships, the IPT shall make use of the NAVSEA shipboard and integrated topside design (ITD) processes for the integration requirements to achieve optimal product performance per reference (a). See the Defense Acquisition Guidebook for implementation requirements for all DON programs.

7.1.14.2 Integrated Technical Information Database

PMs should, when practicable, develop an integrated technical information database for use among operational, maintenance, logistics, supply, and training users. This database will facilitate the sharing of design, engineering, manufacturing, production, and logistics support information thereby reducing duplication and life-cycle support costs. This database should be compatible with other technical information databases of programs within the same SoS or FoS. The Naval Safety Center maintains a mishap database that may be used in order to identify safety and health risks associated with legacy systems.

7.1.15 Modeling and Simulation (M&S)

See the Defense Acquisition Guidebook for implementation guidance for all DON programs.

7.1.16 Software Management

The milestone decision authority (MDA) should provide specific mandatory software management implementation requirements for all DON ACAT programs.

7.1.17 Commercial-Off-The-Shelf (COTS) Considerations

Each introduction of a COTS-based increment of capability, developed under an evolutionary acquisition strategy, should be sustained by logistics support that has been specifically tailored to meet warfighter-specified levels of performance for that increment. Support-related COTS considerations include ease and transparency of operation and maintenance, safety, security capabilities, configuration control of unique aspects, follow-on technology infusion, implications for human systems integration, adequacy of function and/or measurement capability for the intended application, ability of the Navy maintenance infrastructure or contractor support to properly maintain or calibrate COTS equipment and contribution to cost effectiveness.

Integration of COTS items into a system can cause unexpected safety hazards and ESOH risks. As all commercially available items are not necessarily developed to the same safety standards applied in the DoD acquisition process, there is an increased potential for failures that can result in system failures/losses and personnel deaths/injuries. The PM must address the COTS items’ system safety and software engineering considerations that impact procurement, integration, test, and sustainment, and as a result should ensure that environment, safety, and health-related documentation is available for assessing potential hazards or risks.

7.1.18 Metric System

The metric system of measurement is the preferred system of weights and measures for all elements of defense systems requiring new design, unless the PM determines that it is impractical or is likely to cause significant inefficiencies or loss of markets to United States firms (15 U.S.C. Sections 205a-205k and Executive Order 12770). Each SYSCOM, PEO, and DRPM is responsible for administration of the metrication program.

7.1.19 Value Engineering

Value engineering may be less applicable when a program is using COTS hardware. See the Defense Acquisition Guidebook for implementation guidance for all DON ACAT programs.

7.1.20 Accessibility Requirements

National security systems as defined by Section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. Section 1452) are exempt from the accessibility requirements of Section 508 of the Rehabilitation Act of 1973 (see 29 U.S.C. Section 794d(a)(5)) as amended by the FY 2001 Appropriation for Military Construction (see Public Law 106-246, Section 2405, of July 13, 2000). See the Defense Acquisition Guidebook for accessibility guidance for all other DON electronic and information technology programs.

7.1.21 Government-Industry Data Exchange Program (GIDEP)

Reference (m) provides specific Navy requirements and procedures for participation in the GIDEP program.

COMNAVSEASYSCOM is responsible for budgeting and coordinating the GIDEP program for DON Systems Commands.

The Deputy Assistant Secretary of the Navy (Research, Development and Acquisition) Acquisition and Logistics Management (DASN(ALM)) is designated as the PM for the GIDEP program.

7.2 Human Systems Integration (HSI)

HSI is composed of the systems engineering process and program management efforts that provide integrated and comprehensive analysis, design and assessment of requirements, concepts, and resources for system manpower, personnel, training, human factors engineering (HFE), system safety, occupational health, personnel survivability, and habitability. HSI includes the methods, models, hardware/software tools, management and operating processes, documentation, system design features, and data for integrating the human into the system.

The goal of HSI is to influence concept refinements/ technology development, system design, and associated support requirements so that developmental, non-developmental, and

product-improved systems can be operated, maintained, trained, and supported in the most optimized, cost-effective and safest manner.

HSI is based on eight domains that are intimately and intricately interrelated and interdependent and must be among the primary drivers of effective, affordable, and safe system designs. HSI integrates and facilitates trade-offs among these eight domains, but does not replace individual domain activities, responsibilities, or reporting channels. HSI domains are described as follows.

1. Manpower. The numbers of personnel (military, civilian and contractor) required, authorized and potentially available to operate, maintain, train, administer, and support each capability and/or system.

2. Personnel. The human knowledge, skills, abilities, aptitudes, competencies, characteristics, and capabilities required to operate, maintain, train, and support each capability and/or system in peacetime and war.

3. Training. The instruction, education and resources required to provide Navy personnel with requisite knowledge, skills, and abilities to properly operate, maintain, train, and support Navy capabilities and/or systems.

4. Human Factors Engineering. The comprehensive integration of human characteristics and capabilities and limitations into system definition, design, development, and evaluation to promote effective human-machine integration for optimal total system performance.

5. System Safety. System safety is the systems engineering process involving hazard identification, risk evaluation, design analysis, hazard mitigation/control and management. The process manages the design and operational characteristics of a system that eliminate or minimize the possibilities for accidents or mishaps caused by human error or system failure.

6. Occupational Health. The systematic application of biomedical knowledge, early in the acquisition process, to identify, assess, and minimize health hazards associated with the system's operation, maintenance, repair, or storage.

7. Personnel Survivability. The characteristics of a system that reduce the risk of fratricide and personal detection or targeting, prevent personal attack if detected or targeted, increase survival and prevent injury if personally attacked or

located within an entity being attacked, minimize medical implications if wounded or otherwise injured, and minimize physical and mental fatigue.

8. Habitability. System characteristics that provide living and working conditions which result in levels of personnel morale, safety, health, and comfort adequate to sustain maximum personnel effectiveness to support mission performance and avoid personnel retention problems.

7.2.1 HSI in Acquisition

HSI is initiated early in the acquisition process and implemented as described in the acquisition strategy. Where full capability will be achieved through evolutionary acquisition increments or pre-planned product improvement modifications, the long-term strategy for achieving HSI requirements within each increment or modification should be discussed as part of the overall acquisition strategy. PMs are encouraged to coordinate with CNO (N12 and N09FB) on the development of the HSI approach for each increment or modification. See reference (a) for further guidance and direction.

7.2.2 Manpower, Personnel, and Training (MPT)

MPT concepts should be consistent with the Navy Total Force Strategy as described in reference (n).

7.2.2.1 Manpower and Personnel

Based on functional analysis, an assessment will be conducted to determine the extent to which functions should be automated, eliminated, consolidated, or simplified. Manpower, personnel, and training concepts should be consistent with the Navy Total Force Strategy as described in reference (n). The PM shall take advantage of other system and mission area personnel initiatives that resulted in applicable personnel advantages per reference (o).

7.2.2.2 Training

The Training System Plan (TSP) should provide manpower, personnel, and training (MPT) alternatives in support of the ACAT program’s thresholds and objectives. Individual system and platform training requirements shall be developed in close collaboration with development of related systems throughout the acquisition process to increase training efficiency, identify commonalities, merge training requirements, and avoid duplication per reference (a).

The TSP identifies MPT needs, concepts, strategies, constraints, risks, data, resources, and also guides MPT program and budget submissions. References (a) and (p) for Navy programs, require the TSP. The resource sponsor approves the

TSP. Navy TSPs are approved after concurrence by CNO (N1). All programs shall develop a TSP. An initial TSP should address the MPT concepts. Development of the TSP is the responsibility of the PM. CNO (N1) shall validate functional and/or workload methodology utilized to define manpower and personnel requirements contained in the Navy TSP per reference (p). Additional guidance on the Navy TSP can be found in reference (p) and accompanying guides/manuals.

Training analyses shall be conducted as part of the overall systems engineering process to identify options for individual, collective, and joint training for operators, maintainers, and support personnel, and to identify tasks for training, tasks for which training is unnecessary and tasks for which Job Performance Aids and Electronic Performance Support Systems can maximize task efficiency and accuracy per references (p) and (q). In addition, the analyses shall identify tasks for which performance should be designed into the system to minimize the amount of training required, minimize task overload and maximize efficiency and accuracy of the performer per references (p) and (q). The analyses shall review processes to simplify tasks, minimize dependency on memory, and optimize for knowledge management per reference (p). Training decisions shall be based on the results of front-end and media analyses, with consideration given to the types of knowledge and skills to be taught and the application of instructional design principles per reference (p). Poor design and un-mitigated safety hazards are potential contributors to increased training requirements and costs. These can be minimized through early planning and integration with HFE and system safety.

7.2.3 Human Factors Engineering (HFE)

The purpose of HFE is to achieve system performance, MPT, maintenance, and habitability requirements, as well as mitigate safety and health hazard issues. It shall encompass functional analysis and allocation of functions and technology requirements to support functional allocation concepts, and M&S to further develop and evaluate alternative concepts for addressing human roles, responsibilities and requirements in system performance per reference (a). An acquisition, design, or development approach shall consider system integration as one of the initial steps in design per reference (a). Human involvement should be justified through a function and task analysis that can be used as a basis to make human-machine allocation decisions. The goal is to reduce/eliminate redundancy, optimize task allocation and information flow, and ensure an efficient and cost-effective process throughout the system. The HFE considerations for system design will extend to job procedures, job aids, and decision support systems. The HFE effort will also emphasize design activities required to ensure quality of service, including quality of life and quality of work. Opportunities for cost savings and mission enhancement include materials handling,

maintenance functions, human, sensor, and computer interface, walking and working surfaces (safety), and design for most efficient access. The design should minimize human performance errors, interface problems, and workload (physical, cognitive, attention) requirements.

7.2.4 Personnel Survivability

Waivers that affect health and safety should be reviewed by a system safety process per reference (q) and evaluated at a management level consistent with the risk.

7.2.5 Habitability

See reference (a) for guidance and direction.

7.3 Environmental, Safety, and Occupational Health (ESOH)

ASN(I&E) advises ASN(RD&A) on ESOH issues, to include review and comment on or endorsement of National Environmental Policy Act (NEPA) or Executive Order (EO) 12114 environmental documents (see the tables in reference (a)).

Balancing the elimination or reduction of ESOH hazards and associated risk with an informed and structured residual risk acceptance process is essential for positively contributing to a program's efforts in meeting cost, schedule, and performance requirements. ESOH risks are part of each program’s overall cost, schedule, and performance risks and the program should review them from within that overall context. The ESOH risk management process uses ESOH risk analysis matrices, based on the guidance in MIL-STD-882D. The risk matrices should use clearly defined probability and severity criteria (either qualitative or quantitative) to categorize ESOH risks. PMs elect to either establish a single consolidated ESOH risk matrix or use individual environmental, safety, and occupational health matrices.

The three basic types of ESOH risks are:

1. Potential ESOH impacts and adverse effects from routine system development, testing, training, operation, sustainment, maintenance, and demilitarization/disposal.

2. Potential ESOH and mission readiness impacts from system failures or mishaps, including critical software failures.

3. Potential impacts to program life-cycle cost, schedule, and performance from ESOH compliance requirements.

Safety consists of those system design characteristics that serve to minimize the potential for mishaps causing death or injury to operators and maintainers or threaten the survival and/or operation of the system. Prevalent issues include factors

that threaten the safe operation and/or survival of the platform, control of hazardous energy release-mechanical, electrical, fluids under pressure, ionizing and non-ionizing radiation (often referred to as "lock-out/tag-out"), walking and working surfaces including work at heights, fire and explosion and pressure extremes.

System safety analyses should address hardware, software, and people as appropriate from design through operation, sustainment, and disposal. System safety tools will also be used to qualify and quantify environmental protection risks and results of such ESOH analyses and residual risk acceptance should be summarized in the programmatic ESOH evaluation (PESHE).

Occupational health hazards are system design features that create risks of injury, acute or chronic illness, disability, and/or reduce job performance of personnel who operate, maintain, or support the system. Prevalent issues include acoustic energy (noise), biological substances, chemical safety, atmospheric hazards (including those associated with confined space entry and oxygen deficiency), shock and vibration, ionizing and non-ionizing radiation, human factors issues that can create chronic disease and discomfort such as repetitive motion diseases and temperature extremes. Many occupational health problems, particularly noise and chemical substance management, overlap with environmental impacts. Human factors stresses that create risk of chronic disease and discomfort overlap with HSI and HFE considerations. The PESHE describes how ESOH risks are managed, how ESOH and HSI efforts are integrated, and summarizes the ESOH risk information (hazard identification, risk assessment, mitigation decisions, residual risk acceptance, and evaluation of mitigation effectiveness).

There is no specific format for the PESHE. The PM documents the PESHE in whatever manner is most useful to the program and best communicates to decision makers ESOH issues affecting the program. The PESHE also summarizes the ESOH of the system, discusses the approach for integrating ESOH considerations into the systems engineering process, identifies ESOH responsibilities, provides a method for tracking progress, and includes a schedule for NEPA and EO 12114 compliance. During system design, the PM documents hazardous material used in the system and plans for the system’s demilitarization and disposal. The PESHE is required for all programs, regardless of ACAT. Prior to submittal, CNO N45 and CNO N009FB should review the PESHE. The PESHE is required at Program Initiation for ships, Milestone B (for all programs) with an update for MS C and Full-Rate Production Decision Review. Development of the PESHE is the responsibility of the PM. Additional guidance on the PESHE can be found in the Defense Acquisition Guidebook.

Reference (q) does not require that the PESHE supersede or replace other ESOH plans, analyses, and reports (e.g., System Safety Management Plan/Assessments, Hazardous Material (HAZMAT)

Management Plan, Pollution Prevention Plan, Health Hazard Assessments, etc.); the PM incorporates the information provided by these documents by reference, as appropriate. However, to the maximum extent possible, the PM should minimize duplication of effort and documentation and give preference to recording ESOH information in the PESHE, as opposed to maintaining a series of overlapping, redundant documents. HSI also addresses many of the safety and health ESOH areas. The PESHE describes the linkage between ESOH and HSI and how the program avoids duplication of effort.

7.3.1 ESOH Compliance

See reference (a) for guidance and direction.

7.3.2 National Environmental Policy Act (NEPA) and Executive Order (EO) 12114 Environmental Effects Abroad

The NEPA and EO 12114 compliance schedule includes events or proposed actions (to include T&E and fielding/basing activities) throughout the program’s life-cycle. The proponent for each proposed action having the lead to prepare the formal NEPA documentation, establishes the initiation date for each action, establishes the type of NEPA/EO 12114 documentation prior to the proposed action start date, establishes the start and completion dates for the final NEPA/EO 12114 documentation, and identifies the specific approval authority.

The PEO, SYSCOM Commander, DRPM, PM, or designees, and other action proponents are responsible for environmental planning, budgeting, and compliance with environmental requirements for DON acquisition and non-acquisition programs. Preparation of applicable NEPA and EO 12114 documentation is considered an integral part of planning for testing, production, and deployment. Environmental planning process should be initiated at the outset of new program planning. Fleet Commanders are action proponents for decisions involving deployment or fielding of DON systems. COMOPTEVFOR or Director, MCOTEA, or designees, are action proponents for dedicated OT&E. CNR, or designee, is an action proponent for S&T projects and actions. Action proponents shall consider and document the potential to affect the human and natural environment before decisions that could affect the human and natural environment are made per reference (a). As part of NEPA process, alternatives must be considered including alternative sites. Reference (r) provides DON policy for selecting sites per NEPA and EO 12114.

7.3.3 Safety and Health

See references (a), (s), and (t) for guidance and direction.

7.3.4 Hazardous Materials Management

Per reference (u), a hazardous material is defined as anything that, because of its quantity, concentration, or chemical, biological, or physical characteristics, may pose substantial hazard to human health of the environment and generate ESOH-related concerns that result in an elevated level of effort to manage. This definition includes materials that may be used in manufacturing, operations, maintenance, and disposal over a system's life-cycle, which may result in the release of hazardous materials.

Hazardous materials management includes maintaining the following risk information: locations and quantities of hazardous material in the system, energetic qualification information for each energetic material used in the system, reasonably anticipated hazardous byproducts/discharges and expected quantities of hazardous waste generated during normal use/maintenance as well as during emergency situations, special hazardous material training and handling requirements, and demilitarization and disposal requirements. The preferred mitigation strategy is source reduction or elimination of the hazards, also referred to as pollution prevention. References (v) and (w) set forth policy and uniform procedures for demilitarization and disposal of DoD property. Authorization for Navy and Marine Corps possession and use of radioactive material is granted by Naval Radioactive Material Permits issued by the Naval Radiation Safety Committee. Products used in maintenance of weapons systems and related support equipment and facilities account for approximately 80 percent of the hazardous materials and related waste generated by DoD. Thus, design for use of the least hazardous materials and process consistent with efficiency and mission performance provides enormous opportunities for risk management and life cycle cost avoidance.

7.3.5 Pollution Prevention

The PM should consider pollution prevention methods, practices, and technologies early in the program to mitigate ESOH, cost, and schedule risks. Pollution prevention should be an integral part of systems engineering throughout the life-cycle of the program.

The DoD Green Procurement Program (GPP) applies to all acquisitions from major systems programs to individual unit supply and service requisitions. The purpose of the GPP is to enhance and sustain mission readiness through cost effective acquisition that achieves compliance and reduces resource consumption and solid and hazardous waste generation. Consistent

with requirements of Federal procurement preference programs, green products or services must be considered as the first choice in all procurements including, but not limited to the following categories: office products, printing services, Fleet maintenance products, building construction, renovation and maintenance, traffic control, park and recreation, appliances, and lighting. In every procurement action, the procurement request originator must justify a decision not to procure a green alternative per the requirements of Federal green procurement preference programs. See USD(AT&L) memorandum of 27 Aug 04, "Establishment of the DoD Green Procurement Program" and ASN(RD&A) memorandum 22 Nov 04 GPP, "Department of Defense (DoD) Green Procurement Program (GPP)."

7.3.6 Explosives Safety

All ship installations of new or modified weapons, or weapons systems, shall be formally reviewed and approved for safety during the System Development and Demonstration phase per reference (a). Weapons and explosives risks shall be identified and managed using the process identified in reference (x), and shall be briefed to the Navy's Weapons System Explosives Safety Review Board (WSESRB) per reference (y).

7.3.7 Aviation Critical Safety Items (CSIs)

Aviation Critical Safety Items (CSIs) are parts whose failure would have catastrophic consequences to the aircraft, unmanned air vehicles, aircraft launch and recovery equipment, aviation weapons and equipment, and associated aviation support equipment in which they are used. CSIs represent less than five percent of the total population of replenishment parts used in aviation systems, but the implications of failure require that they be identified and carefully managed from design through to disposal. Rather than repeat existing and proposed policies, the below provides source information and summaries of key aviation CSI statutes, regulations, instructions, and guidance.

Reference (z) established policy, procedures, and responsibilities for the life-cycle management of items critical to naval aviation safety. Reference (z) standardized terminology, definitions, criteria, and management requirements across the military Services, Defense Logistics Agency (DLA), and Defense Contract Management Agency (DCMA) when they are involved in designing, acquiring, repairing or overhauling, or supporting naval aviation systems and equipment. Reference (aa), Section C8.5, established procedures for controlling aviation CSIs.

Because of concerns regarding proper identification and life-cycle management of CSIs, reference (ab), Section 802 (codified in 10 U.S.C. Section 2319), established the requirement for the Secretary of Defense to prescribe policy for the quality control of aviation CSIs. Specifically, reference (ab), Section 802, required that 1) Design Control Activities establish a

process to identify and manage aviation CSIs; 2) aviation CSIs be purchased only from sources approved by the Design Control Activity; and 3) delivered aviation CSIs meet requirements established by the Design Control Activity. As defined by reference (ab), Section 802, the Design Control Activity is the systems command of a military department specifically responsible for ensuring the airworthiness of an aviation system or equipment in which aviation CSIs will be used. Additionally, Public Law 108-87 (Department of Defense Appropriations Act, 2004; 30 Sep 2003), Section 8143, required the Secretary of Defense to report on the Department of Defense's process to track defective parts that were potentially safety-critical and the DoD's standards to ensure timely notification of contracting offices and contractors regarding defective safety-critical parts.

7.3.8 Corrosion Prevention and Control

At the time of program initiation, the PM should identify the corrosion susceptibility of the prospective system. For all programs deemed 'corrosion susceptible', the following should apply. The PM should establish a corrosion prevention and control program that identifies attributes of the system's design and construction that are likely to facilitate or exacerbate corrosion during operational use. The PM should adopt environmentally-compliant materials selection and corrosion prevention techniques during the design and manufacture of weapon systems. The PM may prepare a Life Cycle Corrosion Management Plan early in the program life cycle (during phase B). Elements of such a plan may include, as appropriate:

1. Materials and processes selection for corrosion performance and life cycle costs

2. Corrosion mapping of deployed assets to better manage and mitigate corrosion

3. Detecting and correcting corrosion to avoid unnecessary rework and overhaul

4. Preventative inspection requirements at each level of maintenance

5. Advanced planning for the insertion of new corrosion prevention technologies

6. Training and qualifying personnel in corrosion cleaning, repairs, assessment, identification, treatment, preservation, lubrication, hazardous waste disposal, and reporting.

Guidance for corrosion prevention and control is available in a DASN(RD&A)ACQ Technical Bulletin - "*Corrosion Prevention and Detection*" which can be found at http://acquisition.navy.mil/content/view/full/1387. See the Defense Acquisition Guidebook for implementation guidance for all DON ACAT programs.

Annex 7-A

Systems Engineering Plan (SEP) Signature Pages

SEP Approval Page for ACAT ID/IAM programs

SEP Coordination Page for ACAT ID/IAM programs

SEP Coordination/Approval Page for ACAT IC/IAC/II/Special Interest programs

SEP Coordination/Approval Page for ACAT III/IV programs

Systems Engineering Plan (SEP) Signature Pages

SEP Approval Page For ACAT ID/IAM Programs

[PROGRAM NAME – ACAT LEVEL]

SYSTEMS ENGINEERING PLAN (SEP)

VERSION: _____

SUPPORTING MILESTONE: _____

MONTH DAY, YEAR: _____

OSD APPROVAL:

_____ _____
Name Date
Milestone Decision Authority
or Designated SEP Approval Authority

Distribution is limited to U.S. Government agencies only. Other requests for this document must be referred to the ASN(RD&A) Chief Systems Engineer.
CLASSIFIED BY:_____
DECLASSIFY ON:_____

SEP Coordination Page For ACAT ID/IAM Programs

[PROGRAM NAME – ACAT LEVEL]

SYSTEMS ENGINEERING PLAN

VERSION: _____

SUPPORTING MILESTONE: _____

MONTH DAY, YEAR: _____

SUBMITTED BY:

Name Lead/Chief Engineer	Date	Name Program Manager	Date

CONCURRENCE:

Name SYSCOM Chief Engineer	Date	Name PEO/SYSCOM/DRPM	Date

COMPONENT APPROVAL:

Name ASN(RD&A) Chief Systems Engineer	Date

Distribution is limited to U.S. Government agencies only. Other requests for this document must be referred to the ASN(RD&A) Chief Systems Engineer.
CLASSIFIED BY:_____
DECLASSIFY ON:_____

SEP Coordination/Approval Page For ACAT IC/IAC/II/Special Interest Programs

[PROGRAM NAME – ACAT LEVEL]

SYSTEMS ENGINEERING PLAN (SEP)

VERSION: _____

SUPPORTING MILESTONE: _____

MONTH, DAY YEAR: _____

SUBMITTED BY:

_____		_____	
Name	Date	Name	Date
Lead/Chief Engineer		Program Manager	

CONCURRENCE:

_____		_____	
Name	Date	Name	Date
SYSCOM Chief Engineer		PEO/SYSCOM/DRPM	

APPROVAL:

_____	
Name	Date
ASN(RD&A) Chief Systms Engineer	

Distribution is limited to U.S. Government agencies only. Other requests for this document must be referred to ASN(RD&A) Chief Systems Engineer.
CLASSIFIED BY:_____
DECLASSIFY ON:_____

SEP Coordination/Approval Page For ACAT III/IV Programs

[PROGRAM NAME – ACAT LEVEL]

SYSTEMS ENGINEERING PLAN (SEP)

VERSION: _____

SUPPORTING MILESTONE: _____

MONTH, DAY YEAR: _____

SUBMITTED BY:

Name Lead/Chief Engineer	Date	Name Program Manager	Date

CONCURRENCE:

Name SYSCOM Chief Engineer	Date	Name PEO/SYSCOM/DRPM	Date

APPROVAL:

Name Milestone Decision Authority	Date

Distribution is limited to U.S. Government agencies only. Other requests for this document must be referred to ASN(RD&A) Chief Systems Engineer.
CLASSIFIED BY:_____
DECLASSIFY ON:_____

Chapter 8
Acquisition of Services

8.1 Introduction

8.2 Applicability

8.3 Definitions

8.4 Responsibilities

8.5 Review and Approval Thresholds

8.6 Review Procedures

8.7 Outcomes

8.8 Metrics

8.9 Data Collection

8.10 Execution Reviews

8.11 Decision Authority Acquisition Management Responsibilities

Chapter 9
Program Management

References: (a) SECNAVINST 5420.188F

9.1 Assignment of Program Executive Responsibilities

9.2 International Cooperative Program Management

Participation in international cooperative programs requires the establishment of an international agreement. International agreements normally include details of financial arrangements, security considerations and procedures, program management structure, use and disclosure of information between participants, and sales and transfers of information and equipment to third parties. Staffing of international agreements and supporting documentation will include coordination with appropriate financial, legal, and international policy agencies/offices, and will be managed by Navy International Program Office (IPO). Program proponents should consult with Navy IPO for guidance on the latest policies and procedures for developing and implementing international agreements.

9.3 Joint Program Management

For joint programs, an operating agreement will be prepared and should identify responsibilities for funding, participation in joint program decision-making, program information/documentation preparation, endorsement, and approval and other topics as appropriate.

When a DON activity is considering involvement in another service program that is past the Full-Rate Production Decision Review, and when there has been no previous formal involvement, the decision to forward funds to the lead service will be supported by:

1. Program Information/Documentation. Other Service or agency program information/documentation supported by a DON endorsement will be used to the maximum extent possible. Any unique DON activity requirements will be addressed in supporting documentation.

2. Decision. The information/documentation requirements to support the DON activity's decision to participate in other Services' or agencies' programs will follow the general guidelines of reference (a).

Chapter 10
SECNAVINST, OPNAVINST, and Marine Corps Orders Cancellations

The following SECNAV, OPNAV, and Marine Corps issuances were incorporated in and canceled by SECNAVINST 5000.2C of 19 Nov 04:

SECNAVINSTs/Notices/Memorandums

Issuance	Subject
SECNAVINST 5000.2B,	Implementation of Mandatory Procedures for Major and Non-Major Defense Acquisition Programs and Major and Non-Major Information Technology Acquisition Programs, of 6 Dec 96
ASN(RD&A) memorandum,	Revision to Acquisition Program Baseline Format, of 17 Mar 00
ASN(RD&A) memorandum,	Navy Implementation of Department of Defense Policy on Specifications And Standards Reform, of 21 Dec 94
ASN(RD&A) memorandum,	Implementation of Department of Defense Policy on Specifications and Standards, of 27 Jul 94
DASN(ACQ) memorandum,	Acquisition of Services, of 10 Mar 03
DASN(ACQ) memorandum,	Promulgation of DoD 5000 Directive and Instruction, of 9 Jun 03

OPNAVINSTs

Issuance	Subject
None	

Marine Corps Orders (MCOs)

Issuance	Subject
None	

Chapter 11
Glossary

This glossary contains terms used in SECNAVINST 5000.2D. Entries are in alphabetical order. In some cases the reader is referred to other instructions where a fuller discussion is already provided.

Abbreviated Acquisition Program (AAP)

- a weapon system program: (1) whose cost is less than all of the following dollar thresholds: $10 million in total development cost for all fiscal years, $25 million in total production or services cost for any fiscal year, and $50 million in total production or services cost for all fiscal years, (2) which does not affect the military characteristics of ships or aircraft or involve combat capability, (3) which does not require an operational test and evaluation, and (4) is so designated by the cognizant PEO/SYSCOM Commander/DRPM.

- an information technology program: (1) whose cost is less than all of the following dollar thresholds: $15 million in program costs for any single year and $30 million in total program costs, (2) which does not require an operational test and evaluation, and (3) is so designated by ASN(RD&A) or designee, or PEO/SYSCOM Commander/DRPM.

Acquisition Category IV - a program not meeting the criteria for ACAT I, II, or III. ACAT IVT programs require Operational Test and Evaluation (OT&E). ACAT IVM programs are monitored by COMOPTEVFOR or Director, MCOTEA, but do not require OT&E.

Acquisition Coordination Team (ACT) - a team, normally composed of representatives of the requirements generation, acquisition, testing and financial communities, required for ACAT I and II programs. The ACT is specifically used to oversee the analysis of alternatives, form a tailoring agreement proposal (for program documentation and structure), develop an acquisition strategy and resolve issues at the lowest level possible. ACT’s are encouraged, but not required, for ACAT III and IV programs. See SECNAVINST 5420.188 series.

Acquisition Program Baseline (APB) - a document that contains the cost, schedule and performance objectives and thresholds of the program beginning at program initiation. It contains only the most important parameters that, if the thresholds were not met, the MDA would require a reevaluation of alternative concepts or design approaches.

Acquisition Review Board (ARB) - the senior-level forum for advising the PEO/SYSCOM/DRPM on critical decisions concerning all ACAT I and II programs prior to proceeding to a program decision meeting (PDM) with ASN(RD&A). For ACAT III and IV programs, the

ARB serves as the program decision point meeting. The ARB is chaired by the PEO/SYSCOM/DRPM and participation is determined by the milestone decision authority. Representatives of the CNO/CMC are also invited to participate.

Acquisition Strategy (AS) - an acquisition strategy documents a program manager's (PM's) top-level business and technical management strategy to achieve life-cycle program objectives within the resource constraints imposed. It is the framework for planning, directing, contracting, and managing a program. It provides a program structure and master schedule of events for technology development, system development and demonstration, test and evaluation, production and deployment, operations and support, other activities essential for program success, and is the basis for formulating program plans. See enclosure (3), paragraph 3.4, of this guidebook for elements of an acquisition strategy.

Acquisition Plan (AP) - an acquisition plan documents the acquisition planning required to develop, test, and procure program end items and the support services for such end items. An acquisition plan is required by Part 7 of the Federal Acquisition Regulation (FAR) and by Part 207 of the Defense Federal Acquisition Regulation Supplement (DFARS) above certain dollar thresholds defined therein. An acquisition plan may be a stand-alone plan, may be part of an acquisition strategy, or may be part of a single acquisition management plan (SAMP) as long as all of the requirements of the FAR, DFARS, and the Navy-Marine Corps Acquisition Regulation Supplement (NMCRS) are satisfied.

Advanced Concept Technology Demonstration (ACTD) - a means of demonstrating the use of mature technology in a system to address urgent military needs. The ACTD is not an acquisition program but if additional units beyond the capability created are required, the ACTD should be converted into an acquisition program.

Automated Information System (AIS) - an acquisition program that acquires Information Technology (IT), except IT that:

(1) involves equipment that is an integral part of a weapon or weapon system; or

(2) is a tactical communication system.

Critical Application Item (CAI) - an item that is essential to weapon system performance or operation, or the preservation of life or safety of operating personnel, as determined by the military services. The subset of CAIs whose failure could have catastrophic or critical safety consequences are know as Critical Safety Items.

Critical Infrastructure Protection (CIP) - is mission protection and the identification, assessment, and assurance of cyber and

physical infrastructure that support mission critical capabilities and requirements, to include political, economic, technological, and informational security environments essential to the execution of the National Military Strategy.

Critical Safety Item (CSI) - a part, assembly, installation equipment, launch equipment, recovery equipment, or support equipment for an aircraft or aviation weapons system that contains a characteristic any failure, malfunction, or absence of which could cause a catastrophic or critical failure resulting in loss or serious damage to the aircraft or weapons system, an unacceptable risk of personal injury or loss of life, or an uncommanded engine shutdown that jeopardizes safety.

Defense Business System (DBS) - an information system, other than a National Security System, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management.

Developing Agency/Activity (DA) - the PEO, SYSCOM, DRPM, or other organizations assigned responsibility for program execution.

Evolutionary Acquisition (EA) - an acquisition strategy whereby a basic capability is fielded with the intent to procure and field additional capabilities via blocks in the form of modifications to the basic capability fielded. This technique is often found in the development, production and fielding of programs involving rapidly advancing technology and software and with programs involving rapidly changing requirements.

Extension of Application - an acquisition strategy whereby an existing system, subsystem or equipment is selected to be extended in its application to a new host platform. This strategy usually does not require an operational evaluation (OPEVAL) in the new host platform, but a period of follow-on operational test and evaluation (FOT&E) is usually required to ensure that the system, subsystem or equipment integration has not degraded performance, including the performance of the host platform.

Failure Modes, Effects and Criticality Analysis - the analysis of the various ways in which equipment is expected to fail, the failure’s resultant effects, and impact on mission accomplishment.

Family of Systems (FoS) - a set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capability needs. The mix of systems can be tailored to provide desired capabilities dependent on the situation.

FORCEnet - FORCEnet is the Navy and Marine Corps initiative to achieve Net-Centric Operations and Warfare (NCOW) and Joint Transformation by providing robust information sharing and collaboration capabilities across the Naval/Joint force. FORCEnet capabilities are described by the FORCEnet Functional Concept of 7 Feb 05 (SECNAVINST 5000.2D, enclosure (2), paragraph 2.1.2.5).

Habitability - is that military characteristic of Navy ships directed toward satisfying personnel needs which are dependent upon physical environment.

Hazardous Material – material that due to its chemical, physical, or biological nature causes safety, public health, or environmental concerns that elevate efforts to manage.

Health Hazard - any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.

Human Factors Engineering (HFE) - the systems engineering discipline that addresses integration of human characteristics into system definition, design, development, and evaluation to optimize human-machine performance under operational conditions.

Human Systems Integration (HSI) - the integrated and comprehensive analysis, design, and assessment of requirements, concepts and resources for system manpower, personnel, training, safety and occupational health, habitability, personnel survivability, and human factors engineering (HFE).

Information Resources (IR) - information and related resources, such as personnel, equipment, funds, and information technology (44 U.S.C. Section 3502(6)). Excluded are computer resources, both hardware and software, that are: physically part of, dedicated to, or essential in real time to the mission performance of weapons systems.

Information System – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. Section 3502(8)).

Information Technology (IT) - any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

(1) the term "equipment" means any equipment used by a Component directly or is used by a contractor under a contract with the Component that requires the use of the equipment, or the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

(2) the term "IT" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

This "IT" definition is from the Clinger-Cohen Act (Public Law 104-106, 10 Feb 96, Section 5002) (40 U.S.C. Section 1401(3)).

Per 44 U.S.C. Section 3502(9), the term "IT" as defined in the Paperwork Reduction Act (Public Law 104-13), as amended by Public Law 104-106 Section 5605, does **NOT** include National Security Systems as defined in the Clinger-Cohen Act (Public Law 104-106, 10 Feb 96, Section 5142) (40 U.S.C. Section 1452).

Information Technology (IT) System - any system that is an interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, including computers, ancillary equipment, software, firmware and similar procedures, services (including support services), related resources, automated information systems (AISs) such as electronic commerce/electronic data interchange, non-tactical networks, messaging systems, and base level infrastructure.

Information Technology Program - a program that acquires an automated information system (AIS), except AIS that:

(1) involves equipment that is an integral part of a weapon or weapon system; or

(2) is a tactical communication system.

Integration - the process of combining the electrical/electronic/mechanical/human components of a system into an overall system. Also the process of combining systems of a set of systems into a system of systems (SoS) (adapted from IEEE Standard 610.12-1990).

Interoperability - (1) the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to make use of the services, units, or forces and to use the services so exchanged to enable them to operate effectively together. (2) the condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their

users. (3) the ability of hardware to physically and mechanically interface, operate with, and support other hardware. The degree of interoperability should be defined when referring to specific cases.

Joint Potential Designator - a categorization indicating the degree to which a program has potential for joint use. The codes are: joint, joint interest, or independent.

Level of Repair Analysis - the analysis of a repairable item to determine whether organizational, intermediate or depot is the most appropriate level of repair.

Maintenance Concept - expresses the overall maintenance plan for maintaining the platform and system at a defined level of material readiness in support of the operational scenario. It includes preventive maintenance, corrective maintenance and depot-level maintenance. It should consider maintainability at all maintenance levels (i.e., organizational, intermediate, and depot) as well as address the scope of required work at each level.

Maintenance Releases - maintenance releases are "fixes" for minor problems and will not require testing by COMOPTEVFOR. However, COMOPTEVFOR testing is appropriate when maintenance releases are so numerous as to jeopardize the reliability and performance of the software. In such cases, COMOPTEVFOR will determine the need and extent of operational testing and inform the DA, with an information copy to CNO (N091) and program sponsor.

Major Automated Information System (MAIS) Acquisition Program - a program estimated by the Assistant Secretary of Defense (Networks and Information Integration) (ASD(NII)) to require program costs for any single year in excess of $32 million (FY 2000 constant dollars), total program costs in excess of $126 million (FY 2000 constant dollars), or total life-cycle costs in excess of $378 million (FY 2000 constant dollars), or those otherwise designated by the ASD(NII) to be ACAT IA. ACAT IA programs have two sub-categories (ACAT IAM and IAC).

Major Contract - a contract that is greater than $50 million in then-year dollars (DODI 5000.02, enclosure 4, Table 4).

Major Defense Acquisition Program - a program estimated by the Under Secretary of Defense (Acquisition, Technology and Logistics) (USD(AT&L)) to require eventual expenditure for research, development, test, and evaluation of more than $365 million (Fiscal Year (FY) 2000 constant dollars) or procurement of more than $2.190 billion (FY 2000 constant dollars), or those otherwise designated by the USD(AT&L) to be ACAT I. ACAT I programs have two sub-categories (ACAT ID and IC).

Major Releases - major software releases will require operational testing either as full OT&E or FOT&E by COMOPTEVFOR. Such

releases involve a change that adds new functions or warfare capabilities, interfaces with a different weapon system, redesigns the software architecture, ports the software to a new hardware platform, or rewrites the software in different language.

Manpower Requirements - the number and type of personnel (military, civilian, or contractor) required and potentially available to operate, maintain, support, and provide training for systems per 10 U.S.C. Section 2434.

Measure of Effectiveness (MOE) - the operational performance parameter that specifies a mission area capability or characteristic as identified in the capability development/production document (CDD/CPD).

Measure of Performance (MOP) - testable parameters that relate directly to a MOE such that the effect of a change in the MOP can be related to change in the MOE. MOPs are identified in the test and evaluation master plan (TEMP).

Minor Releases - minor releases are improvements that do not add any new functions, warfare capability, or interfaces and do not meet any of the criteria of a major release. The content and scope of minor releases will be reviewed by Commander, Operational Test and Evaluation Forces (COMOPTEVFOR) for operational testing requirements using the OSD Director, Operational Test and Evaluation (DOT&E) guidelines for operational testing of software. COMOPTEVFOR will determine the need for and extent of operational testing and inform the DA, via message, with an information copy to CNO (N091) and program sponsor. Numerous minor releases can lead to degraded software reliability and performance, in such cases, OPTEVFOR will determine the need for and extent of operational testing and inform the developing agency/activity (DA), via message, with an information copy to CNO (N091) and program sponsor.

Mission Capability - either a direct warfighting capability or a function that crosses several warfighting capabilities. Two examples, of many, that are direct warfighting capabilities are theater air and missile defense (TAMD) and time critical strike (TCS). Two examples, also of many, that are functions that cross several warfighting capabilities are targeting and command and control (C2).

Mission-Critical Information System - a system that meets the definitions of "information system" and "national security system" the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission-critical shall be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management Information Technology (IT) system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller).) A "Mission-Critical

Information Technology System" has the same meaning as a "Mission-Critical Information System." For additional information, see DOD Instruction 5000.2, Enclosure 4.

Mission-Essential Information System – a system that meets the definition of "information system" that the acquiring DoD Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission-essential shall be made by a DoD Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the Under Secretary of Defense (Comptroller).) A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System." For additional information, see DOD Instruction 5000.2, Enclosure 4.

National Security System - any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which:

(1) involves intelligence activities;

(2) involves cryptologic activities related to national security;

(3) involves command and control of military forces;

(4) involves equipment that is an integral part of a weapon or weapons system;

(5) subject to the limitation below, is critical to the direct fulfillment of military or intelligence missions. **This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).**

This definition is from the Clinger-Cohen Act (Public Law 104-106, 10 Feb 96, Section 5142) (40 U.S.C. Section 1452).

Network Centric – exploitation of advancing technology that moves from an application-centric to a data-centric paradigm – that is, providing users the ability to access applications and services through Web services – an information environment comprised of interoperable computing and communication components (GIG MA ICD).

Net-Centric Warfare (NCW) – an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking

knowledgeable entities in the battle space (GIG ES ICD).

Non-Acquisition Program - an effort that does not directly result in the acquisition of a system, subsystem, or equipment for operational use. Non-acquisition programs are research and development funded which may have some application to an acquisition program in the future. These efforts often provide a proof of principle or technology application. (see SECNAVINST 5000.2D, enclosure (2), paragraph 2.7)

Personnel - the human knowledge, skills, abilities, competencies, characteristics, and capabilities required to operate, maintain, train, and support each capability and/or system in peacetime and war.

Personnel Survivability - the characteristics of a system that can reduce fratricide, detectability, and probability of being attacked, as well as minimize system damage, personnel injury, and cognitive and physical fatigue.

Production Acceptance T&E (PAT&E) - test and evaluation conducted on production items to ensure systems meet contract specifications and requirements.

Program Decision Meeting (PDM) - the Department's senior-level forum for advising the Assistant Secretary of the Navy (Research, Development and Acquisition) on critical decisions concerning ACAT IC and II programs. The PDM is chaired by the ASN(RD&A) and composed of the Department's senior acquisition officials, DON CIO, representatives of the CNO/CMC, and others, as appropriate. See SECNAVINST 5420.188 series.

Program Sponsor - in coordination with the resource sponsor where separately assigned, acts as the user representative and provides explicit direction with regard to mission and operational requirements generation and changes, program funding, and preparation and approval of necessary program documentation and program decision point information.

Rapid Deployment Capability – a tailored process that provides the ability to react immediately to a newly discovered enemy threat, potential enemy threat or to respond to significant and urgent safety situations through special, tailored acquisition procedures.

Resource Sponsor - where separately assigned from the program sponsor, is responsible for program budget development, submission, and management.

Software Intensive System - For a system to be considered software-intensive, its software must be the largest segment with respect to system development costs, or functionality, or development risk, or development time.

The three general classifications of DoD software-intensive systems are:

(1) Embedded Systems
(2) Automated Information Systems
(3) Command, Control, Communications and Intelligence (C3I) Systems. (Defense Acquisition University (DAU) Systems Acquisition Management (SAM) 101 course definition)

Software Qualification Testing (SQT) - post-Full-Rate Production software testing conducted by an independent test agency for the purpose of determining whether a software product is approved for fleet release.

Standardization - a process used to achieve the greatest practicable uniformity of items of supply and engineering practices, to insure the minimum practicable variety of such items and optimum interchangeability of technical information, training, equipment parts, and components.

Supportability - ensuring that support requirements are met by system introduction, and maintained throughout deployment, at or above formal threshold levels. Determining the most cost effective life-cycle cost, including the costs for information, infrastructure, and rapidly acquired and rapidly obsolete technology. Planned and executed concurrently with all other systems engineering, and a primary analysis consideration in acquiring off-the-shelf alternatives.

System Performance Document (SPD) - an acquisition document or specification that includes all of the performance requirements from a system-of-systems (SoS) or family-of-systems (FoS) Capstone Requirements Document and its individual systems' Operational Requirements Documents that may also define the performance of a mission capability package. An SPD may also include an allocation of capstone or mission capability performance down to the subsystem, component, and equipment levels.

System of Systems - a set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole.

System Safety - the application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

T&E Coordination Group - a forum whose purpose is to coordinate and resolve more complex Navy test and evaluation (T&E) issues, including urgent test and evaluation master plan (TEMP) changes. The forum is chaired by CNO (N091) and membership usually includes CNO staff, program manager (PM), OPTEVFOR Assistant Chief of Staff, and ASN(RD&A) program staff (including Chief Engineer and others).

Test and Evaluation Working-level Integrated Product Team (T&E WIPT) - a forum whose purpose is to discuss, coordinate and resolve test planning goals and issues. The forum is chaired by the PM or the PM's designated representative. Membership is flexible but can include CNO representatives, SYSCOM T&E representatives, COMOPTEVFOR staff, ASN(RD&A) staff, OSD and DOT&E staff, and contractors.

Threshold - the value of a baseline parameter that represents the minimum acceptable value which, in the user's judgment, is necessary to satisfy the need. If threshold values are not achieved, program performance is seriously degraded, the program may be too costly, or the program may no longer be timely.

Total Life-Cycle Cost of Ownership - life-cycle ownership cost includes the cost to develop, acquire, operate, support, and dispose of the system and the related logistics infrastructure. Total costs are determined when acquisition plans and strategies make trade-offs to optimize long-term operations and support considerations. These trade-offs consider lowest total cost of ownership over the expected life-cycle. The term Total Life-Cycle Cost of Ownership is also referred to as Total Ownership Cost

Training - instruction and applied exercises for the attainment and retention of skills, knowledge, abilities, and attitudes required to accomplish tasks. (see definition in MIL-HDBK-29612-4A Glossary for Training)

Unit Cost - there are different kinds of unit cost:

Average Procurement Unit Cost (APUC) - is the amount equal to the total procurement cost divided by the total procurement quantity (Defense Acquisition Guidebook, section 2.1.1.1.(6)). The Defense Acquisition Guidebook is currently available on the Internet at http://akss.dau.mil/dag.

Procurement Unit Cost (PUC) - with respect to a major defense acquisition program, means the amount equal to the total of all funds programmed to be available for obligation for procurement for the program, divided by the number of fully-configured end items to be procured (10 U.S.C. Section 2432 - Selected Acquisition Reports).

Program Acquisition Unit Cost (PAUC) - with respect to a major defense acquisition program, means the amount equal to the total cost for development and procurement of, and system-specific military construction for, the acquisition program, divided by the number of fully-configured end items to be produced for the acquisition program (10 U.S.C. Section 2432 - Selected Acquisition Reports).

Weapons/Weapon Systems - all arms, munitions, materiel, instruments, mechanisms, devices, and those components required for their operation, that are intended to have an effect of injuring, damaging, destroying, or disabling personnel or property, to include non-lethal weapons. For purposes of the legal review required by SECNAVINST 5000.2D, weapons do not include launch or delivery platforms, such as, but not limited to, ships or aircraft, but rather the weapons or weapon systems contained on those platforms.

Weapon System Acquisition Program (DON) - an overarching term that applies to a program for acquisition of a weapon system that includes a host platform (e.g., ship or aircraft), missile, weapon, munitions, training system, combat system, subsystem(s), component(s), equipment(s), associated software, or principal items that may be acquired collectively or individually (i.e., all acquisition programs other than information technology acquisition programs).

Chapter 12
List of Acronyms

3-M	Maintenance and Material Management
AAP	Abbreviated Acquisition Program
ACAT	Acquisition Category
ACMC	Assistant Commandant of the Marine Corps
ACO	Administrative Contracting Officer
ACOS	Assistant Chief of Staff
ACT	Acquisition Coordination Team
ACTD	Advanced Concept Technology Demonstration
ADM	Acquisition Decision Memorandum
ADM	Advanced Development Model
AIS	Automated Information System
AO	Action Officer
AoA	Analysis of Alternatives
AP	Acquisition Plan
APB	Acquisition Program Baseline
API	Acquisition Program Integration
ARB	Acquisition Review Board
ARE	Acquisition Reform Executive
AS	Acquisition Strategy
ASN(FM&C)	Assistant Secretary of the Navy (Financial Management and Comptroller)
ASN(I&E)	Assistant Secretary of the Navy (Installations and Environment)
ASN(M&RA)	Assistant Secretary of the Navy (Manpower and Reserve Affairs)
ASN(RD&A)	Assistant Secretary of the Navy (Research, Development and Acquisition)
ASN(RD&A) CHSENG	Assistant Secretary of the Navy (Research, Development and Acquisition) Chief Systems Engineer
AT	Anti-Tamper
ATC	Air Traffic Control
BIT	Built-In Test
BLRIP	Beyond Low-Rate Initial Production
BUMED	Bureau of Medicine
CAE	Component Acquisition Executive (i.e., ASN(RD&A))
CAI	Critical Application Item
CAIG	Cost Analysis Improvement Group
CAIV	Cost as an Independent Variable
CAO	Contract Administration Office
CARD	Cost Analysis Requirements Description
CARS	Consolidated Acquisition Reporting System
C/SSR	Cost and Schedule Status Report
C4I	Command, Control, Communications, Computers and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CBR	Chemical, Biological and Radiological
CCA	Clinger-Cohen Act

CCDR	Contractor Cost Data Reporting
CCP	Consolidated Cryptologic Program
CD	Combat Development
CDD	Capability Development Document
CEB	Chief of Naval Operations Executive Board
CFFC	Commander, Fleet Forces Command
CFR	Code of Federal Regulations
CFSR	Contract Funds Status Report
CG	Commanding General
CHENG	Chief Engineer
CIAO	Critical Infrastructure Assurance Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
CNR	Chief of Naval Research
COE	Common Operating Environment
COI	Critical Operational Issue
CG, MARCORSYSCOM	Commanding General, Marine Corps Systems Command
COMNAVSECGRU	Commander, Naval Security Group
COMOPTEVFOR	Commander, Operational Test and Evaluation Force
COTS	Commercial-Off-The-Shelf
CPD	Capability Production Document
CPR	Contract Performance Report
CRD	Capstone Requirements Document
CSI	Critical Safety Item
DA	Developing Activity
DAA	Designated Approval Authority
DAB	Defense Acquisition Board
DAES	Defense Acquisition Executive Summary
DASN	Deputy Assistant Secretary of the Navy
DC	Deputy Commandant
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DII	Defense Integrated Infrastructure
DISA	Defense Information Systems Agency
DISR	Defense Information Technology Standards Registry
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DMI	Data Management and Interoperability
DoD	Department of Defense
DON	Department of the Navy
DOT&E	Director, Operational Test and Evaluation
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities
DRPM	Direct Reporting Program Manager
DT	Developmental Testing
DT&E	Developmental Test and Evaluation
DTIC	Defense Technical Information Center
DTSE&E	Director, Test Systems Engineering and Evaluation
DWCF	Defense Working Capital Fund
E3	Electromagnetic Environmental Effects
EA	Evolutionary Acquisition

EAT	External Airlift Transportation
EC	Electronic Commerce
ECCM	Electronic Counter-Countermeasures
ECM	Electronic Countermeasures
ECP	Engineering Change Proposal
EDI	Electronic Data Interchange
EMC	Electromagnetic Compatibility
EMD	Engineering and Manufacturing Development
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EMV	Electromagnetic Vulnerability
EO	Executive Order
EOA	Early Operational Assessment
ESOH	Environmental, Safety, and Occupational Health
EW	Electronic Warfare
EFDS	Expeditionary Force Development System
FAR	Federal Acquisition Regulation
FCB	Functional Capabilities Board
FCCC	FORCEnet Consolidated Compliance Checklist
FCT	Foreign Comparative Testing
FD	Failure Definition
FEA	Functional Economic Analysis
FET	FORCEnet Enterprise Team
FFR	Full Fleet Release
FIBL	FORCEnet Implementation Baseline
FIP	Federal Information Processing
FITS	FORCEnet Implementation Tool Suite
FMB	Financial Management Branch
FMC	Full Mission Capable
FMECA	Failure Modes, Effects, and Criticality Analysis
FMF	Fleet Marine Forces
FMP	Fleet Modernization Program
FOC	Full Operational Capability
FoS	Family of Systems
FOT&E	Follow-on Operational Test and Evaluation
FRCC	FORCEnet Requirements/Capabilities and Compliance
FYDP	Future Years Defense Program
FYMTP	Five-Year Master Test Plan
GIDEP	Government-Industry Data Exchange Program
GIG	Global Information Grid
GIG MA	Global Information Grid Mission Area
HERP	Hazards of Electromagnetic Radiation to Personnel
HERF	Hazards of Electromagnetic Radiation to Volatile Materials
HERO	Hazards of Electromagnetic Radiation to Ordnance
HFE	Human Factors Engineering
HMCM	Hazardous Material Control Management
HQMC	Headquarters Marine Corps
HSI	Human Systems Integration
IA	Information Assurance
IBR	Integrated Baseline Review
ICD	Initial Capabilities Document
ICE	Independent Cost Estimate
IER	Initial Evaluation Report

ILS	Integrated Logistics Support
IM	Information Management
IMMP	Interim Manpower Management Policy
INSURV	(Board of) Inspection and Survey
IOC	Initial Operational Capability
IOT&E	Initial Operational Test and Evaluation
IPO	International Program Office
IPPD	Integrated Product and Process Development
IPT	Integrated Product Team
IR	Information Resources
IRM	Information Resources Management
IS	Information Systems
ISO	International Organization for Standardization
IT	Information Technology
ITD	Integrated Topside Design
JCIDS	Joint Capabilities Integration and Development System
JPD	Joint Potential Designator
JROC	Joint Requirements Oversight Council
JTA	Joint Technical Architecture
JT&E	Joint Test and Evaluation
KSA	Key System Attributes
KSA	Knowledge, Skills and Abilities
LBTS	Land-Based Test Site
LCC	Life-Cycle Cost
LCL	Life-Cycle Logistics
LFT&E	Live Fire Test and Evaluation
LI	Line Item
LIMSCOPE	Limitation to Scope of Testing
LMI	Logistics Management Information
LORA	Level of Repair Analysis
LRIP	Low-Rate Initial Production
LSA	Logistics Support Analysis
M&S	Modeling and Simulation
MAIS	Major Automated Information System
MARCORSYSCOM	Marine Corps Systems Command
MC	Mission Capable
MC	Mission Critical
MC&G	Mapping, Charting and Geodesy
MCCDC	Marine Corps Combat Development Command
MCEB	Military Communications-Electronics Board
MCIC	Marine Corps Intelligence Center
MCO	Marine Corps Order
MCOTEA	Marine Corps Operational Test and Evaluation Activity
MCTSSA	Marine Corps Tactical Systems Support Activity
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
ME	Manpower Estimate
ME	Mission Essential
METCAL	Metrology and Calibration
METOC	Meteorology and Oceanography
MOA	Memorandum of Agreement
MOE	Measure of Effectiveness

MOP	Measure of Performance
MOP	Memorandum of Policy
MOU	Memorandum of Understanding
MPT	Manpower, Personnel, and Training
MTBOMF	Mean Time Between Operational Mission Failure
NAE	Department of the Navy Component Acquisition Executive
NAPS	Navy Acquisition Procedures Supplement
NATO	North Atlantic Treaty Organization
NAVAIRSYSCOM	Naval Air Systems Command
NAVMAC	Naval Manpower Analysis Center
NAVSEASYSCOM	Naval Sea Systems Command
NCB	Naval Capabilities Board
NCCA	Naval Center for Cost Analysis
NCDP	Naval Capabilities Development Process
NCES	Net-Centric Enterprises Services
NCTS	Naval Computer and Telecommunications Station
NDI	Non-Developmental Item
NDPC	National Disclosure Policy Committee
NEPA	National Environmental Policy Act
NETWARCOM	Network Warfare Command
NIB	Not-to-Interfere Basis
NII	Networks and Information Integration
NISMC	Naval Information Systems Management Center
NIST	National Institute of Standards and Technology
NMCARS	Navy Marine Corps Acquisition Regulation Supplement
NORAD	North American Air Defense Command
NOTAL	Not To All
NPOC	Navy Point of Contact
NRB	Navy Review Board
NSA	National Security Agency
NSS	National Security Systems
NTIA	National Telecommunications and Information Administration
NTSP	Navy Training Systems Plan
OA	Open Architecture
OA	Operational Assessment
O&S	Operating and Support
OASN	Office of the Assistant Secretary of the Navy
OMB	Office of Management and Budget
ONR	Office of Naval Research
OPEVAL	Operational Evaluation
OPNAV	Office of the Chief of Naval Operations
OPREP	Operational Report
OPSEC	Operations Security
OPTEVFOR	Operational Test and Evaluation Force
OSD	Office of the Secretary of Defense
OT	Operational Testing
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
OTC	Operational Test Coordinator
OTD	Operational Test Director
OTRR	Operation Test Readiness Review
OUSD(AT&L)	Office of the Under Secretary of Defense

	(Acquisition, Technology and Logistics)
P3I	Pre-planned Product Improvement
PA&E	Program Analysis and Evaluation
PAPL	Preliminary Allowance Parts List
PAT&E	Production Acceptance Test and Evaluation
PBS	Project Baseline Summary
PDM	Program Decision Meeting
PDR	Program Deviation Report
PDREP	Product Deficiency Reporting and Evaluation Program
PE	Program Element
PEO	Program Executive Officer
PESHE	Programmatic Environmental, Safety, and Occupational Health Evaluation
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POM	Program Objective Memorandum
PPBES	Planning, Programming, Budgeting, and Execution System
PQDR	Product Quality Deficiency Report
PSA	Principal Staff Assistant
PTTI	Precise Time and Time Interval
QRA	Quick Reaction Assessment
R3B	Resources and Requirements Review Board
RADHAZ	Radiation Hazard
RAM	Reliability, Availability, and Maintainability
RD&A	Research, Development and Acquisition
RDC	Rapid Deployment Capability
RDDS	Research and Development Descriptive Summary
RDT&E	Research, Development, Test and Evaluation
RFP	Request for Proposal
RO	Requirements Officer
ROD	Record of Decision
SAR	Selected Acquisition Report
SASCO	Security, Acquisition Systems Protection, Systems Security Engineering, Counter Intelligence, and Operations Security
S&T	Science and Technology
SC	Scoring Criteria
SDD	System Development and Demonstration
SECNAV	Secretary of the Navy
SECR	Standard Embedded Computer Resources
SEO	Software Executive Official
SES	Senior Executive Service
SEW	Space and Electronic Warfare
SI	International System of Units
SIE	Standards Improvement Executive
SME	Subject Matter Expert
SoS	System of Systems
SPAWARSYSCOM	Space and Naval Warfare Systems Command
SPD	System Performance Document
SPI	Single Process Initiative
SPR	Software Problem Reports
SSA	Source Selection Authority

SQT	Software Qualification Testing
STA	System Threat Assessment
SYSCOM	Systems Command
T&E	Test and Evaluation
T&E WIPT	Test and Evaluation Working-level Integrated Product Team
TACP	Technology Assessment and Control Plan
TD	Test Director
TECG	Test and Evaluation Coordination Group
TECHEVAL	Technical Evaluation
TEIN	Test and Evaluation Identification Number
TEMP	Test and Evaluation Master Plan
TIWG	Test Integration Working Group
TLCSM	Total Life Cycle Systems Management
TOC	Total Ownership Cost
TPD	Test Planning Document
TPWG	Legacy term: Test Planning Working Group
TR	Test Report
TRA	Technology Readiness Assessment
TSE&E	Test, Systems Engineering and Evaluation
TSP	Test Support Package
TSP	Training System Plan
TTSP	Test Threat Support Package
UCR	Unit Cost Report
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense (Acquisition, Technology and Logistics)
USJFCOM	United States Joint Forces Command
USMC	United States Marine Corps
USN	United States Navy
USNO	United States Naval Observatory
UTC	Coordinated Universal Time
VAMOSC	Visibility and Management of Operating and Support Costs
VCD	Verification of Corrected Deficiencies
VCNO	Vice Chief of Naval Operations
VIE	Visual Information Equipment
WBS	Work Breakdown Structure
WSA	Warfare Systems Architect
WSE	Warfare Systems Engineer

SECNAV M-5000.2

Stock Number
0516LP1085395