Department of Defense
INSTRUCTION

NUMBER 5000.02T
January 7, 2015
Incorporating Change 8, September 15, 2020

USD(A&S)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive (DoDD) 5000.01 (Reference (a)) and DoDD 5135.02 (Reference (cm)), establishes policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through (cw).

b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

c. Assigns, reinforces, and prescribes procedures for acquisition responsibilities related to cybersecurity in the Defense Acquisition System.

d. Incorporates and cancels Directive-type Memorandum 17-001 (Reference (cl)).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. TRANSITION PLAN. DoD Instruction (DoDI) 5000.02 (Reference (b)) lays the groundwork for operation of the Adaptive Acquisition Framework, which is part of the Defense Acquisition System described in DoDD 5000.01. DoDI 5000.02 will eventually cancel this issuance, which has been renumbered DoDI 5000.02T (Transition) to establish a distinction between the two issuances.

a. This issuance will remain in effect, with content removed as it is cancelled or transitions to a new issuance, as shown in Table 1. When the Adaptive Acquisition Framework realignment is complete, an administrative change to DoDI 5000.02 will cancel this issuance.

b. Each new or reissued acquisition policy document listed in Table 1 will clearly state the content from this issuance it incorporates and cancels.

c. After each issuance's publication, this issuance will be administratively updated to remove the cancelled material and the Summary of Changes will state the title and number of the issuance replacing it.

d. Those parts of this issuance that are cancelled without replacement will be formally coordinated in accordance with DoDI 5025.01 (Reference (cz)) and their cancellation similarly documented.

Table 1. Relationship of DoDI 5000.02T and New Policy

DoDI 5000.02T, Operation of the Defense Acquisition System	**Associated New Policy (Issuances with Lettered Extensions in Development)**
Core Acquisition Policy (Paragraph 6, Procedures)	DoDI 5000.85, "Major Capability Acquisition"
Enclosure 1. Acquisition Program Categories and Compliance Requirements -- Information Requirements Tables	• DoDI 5000.85, "Major Capability Acquisition" • Tables "authorized by DoDI 5000.85…" will be posted on the Adaptive Acquisition Framework website
Enclosure 2. Program Management	• DoDI 5000.85, "Major Capability Acquisition" • DoDI 5010.44, "Intellectual Property," October 16, 2019 has replaced "IP Strategy" (formerly Para 6.a.(4))
Enclosure 3. Systems Engineering	DoDI 5000.UJ, "Engineering"
• Enclosure 4. Developmental Test and Evaluation (DT&E) • Enclosure 5. Operational and Live Fire Test and Evaluation (OT&E and LFT&E)	DoDI 5000.UF, "Test and Evaluation (T&E)"
Enclosure 6. Life-Cycle Sustainment	DoDI 5000.85, "Major Capability Acquisition"
Enclosure 7. Human Systems Integration (HIS)	DoDI 5000.PR, "Human Systems Integration in Defense Acquisition"
Enclosure 8. Affordability Analysis and Investment Constraints	Replaced by direction in §807 of Public Law 114-328

Table 1. Relationship of DoDI 5000.02T and New Policy, Continued

DoDI 5000.02T, Operation of the Defense Acquisition System	**Associated New Policy (Issuances with Lettered Extensions in Development)**
Enclosure 9. Analysis of Alternatives (AoA)	Necessary information is in DoDD 5105.84, "Director of Cost Assessment and Program Evaluation," and the Defense Acquisition Guidance.
Enclosure 10. Cost Estimating and Reporting	Necessary guidance is available in DoDI 5000.73, "Cost Analysis Guidance and Procedures."
Enclosure 11. Requirements Applicable to All Programs Containing Information Technology (IT)	DoDI 5000.82, "Acquisition of Information Technology (IT)"
Enclosure 12. Urgent Capability Acquisition	DoDI 5000.81, "Urgent Capability Acquisition"
Enclosure 13. Cybersecurity in the Defense Acquisition System	• Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) DoDI 5000.CS, "Cybersecurity for Acquisition Decision Authorities and Program Managers" • Under Secretary of Defense for Research and Engineering (USD(R&E)) technology and program protection issuance in development

4. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction and the associated new policy listed in Table 1 provide the detailed procedures that guide the operation of the system.

5. RESPONSIBILITIES

a. Defense Acquisition Executive (DAE). The DAE is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). The DAE will act as the MDA for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. In accordance with DoDI 5000.85 (Reference (dc)), the DAE may delegate authority to act as the MDA to the head of a DoD Component, who may further delegate the authority to the Component Acquisition Executive (CAE). The DAE may also delegate MDA authority to another OSD official as the DAE considers appropriate.

b. MDA. The MDA will establish procedures for assigned programs using this instruction as guidance. MDAs should limit mandatory procedures applicable to all assigned programs so as to not exceed the requirements for MDAPs or MAIS programs and other acquisition programs governed by this instruction or DoDD 5000.01 (Reference (a)). MDAs should tailor regulatory procedures in the document consistent with sound business practice and the risks associated with the product being acquired.

c. Heads of the DoD Components. The DoD Component Head will implement the procedures in this instruction and Reference (a). Component-required procedures will not exceed those specified in this instruction. When necessary, waivers or requests for exceptions to the provisions of this instruction will be submitted to the DAE, the DoD Chief Information Officer (DoD CIO), the Director, Operational Test and Evaluation (DOT&E), or the Director, Cost Assessment and Program Evaluation (DCAPE), via the CAE. Statutory requirements cannot be waived unless the statute permits.

d. Secretaries of the Military Departments. In addition to the responsibilities described in paragraph 5.c., the Secretary of the Military Department acquiring an MDAP will represent the customer (i.e., the DoD Component(s) fielding the system). The Secretary concerned, in coordination with the Chief of the Military Service fielding the system, will balance resources against priorities and ensure appropriate trade-offs are made among cost, schedule, technical feasibility, and performance throughout the life of the program.

e. Chiefs of the Military Services. The Chiefs of the Military Services fielding MDAPs will represent the customer and, with the Secretary of the Military Department acquiring the MDAP, balance resources against priorities and ensure that appropriate trade-offs are made among cost, schedule, technical feasibility, and performance throughout the life of the program. The Chief concerned will advise the MDA on trade-offs before Milestones A and B. As part of the MDA's Written Determination before Milestone A and Certification and Determination before Milestone B (these milestone information requirements are detailed in Reference (dc)), the MDA must determine that the Chief and the Secretary concur with the cost, schedule, technical feasibility, and performance trade-offs that have been made.

6. PROCEDURES. This section was removed through formal coordination and approval of Reference (dc); necessary information can be found in that issuance.

7. RELEASABILITY. **Cleared for public release**. This instruction is available on the Directives Division Website at https://www.esd.whs.mil/DD/.

8. SUMMARY OF CHANGE 8. This change removes:

a. Enclosures 9 and 10 from this issuance.

(1) The required policy language concerning Analysis of Alternatives in Enclosure 9 is included in DoDD 5105.84 (Reference (bp)). The remainder of Enclosure 9 not covered by Reference (bp) is best practices and guidance that are unnecessary or can be found in the Defense Acquisition Guidance.

(2) The needed cost estimating policies from Enclosure 10 are already included in DoDI 5000.73 (Reference (w)).

b. Information in Enclosures 3 and 13 regarding technology and program protection, which has been incorporated by DoDI 5000.83 (Reference (db)) as noted in that issuance.

c. Section 6 and Enclosures 1, 2, 6, and 8, which have all been incorporated and cancelled by Reference (dc).

d. Enclosure 12, which has been incorporated and cancelled by DoDI 5000.81 (Reference (de)).

9. <u>EFFECTIVE DATE</u>. This instruction is effective January 7, 2015.

Frank Kendall
Under Secretary of Defense for
Acquisition, Technology, and
Logistics

J. Michael Gil
J. Michael Gilmore
Director, Operational
Test and Evaluation

Terry Halvorsen
Acting DoD Chief
Information Officer

References

Enclosures
1. Acquisition Program Categories and Compliance Requirements
2. Program Management
3. Systems Engineering
4. Developmental Test and Evaluation (DT&E)
5. Operational and Live Fire Test and Evaluation (OT&E and LFT&E)
6. Life-Cycle Sustainment
7. Human Systems Integration (HSI)
8. Affordability Analysis and Investment Constraints
9. Analysis of Alternatives (AoA)
10. Cost Estimating and Reporting
11. Requirements Applicable to All Programs Containing Information Technology (IT)
12. Urgent Capability Acquisition
13. Cybersecurity in the Defense Acquisition System

Glossary

TABLE OF CONTENTS

PURPOSE 1
APPLICABILITY 1
TRANSITION PLAN 1
POLICY 3
RESPONSIBILITIES 3
Defense Acquisition Executive (DAE) 3
MDA 3
Heads of the DoD Components 4
Secretaries of the Military Departments 4
Chiefs of the Military Services 4
PROCEDURES 4
RELEASABILITY 4
SUMMARY OF CHANGE 8 4
EFFECTIVE DATE 5

REFERENCES 10

ENCLOSURE 1: ACQUISITION PROGRAM CATEGORIES AND COMPLIANCE REQUIREMENTS 15

ENCLOSURE 2: PROGRAM MANAGEMENT 16

ENCLOSURE 3: SYSTEMS ENGINEERING 17
PURPOSE 17
SYSTEMS ENGINEERING PLAN 17
DEVELOPMENT PLANNING 18
SYSTEMS ENGINEERING TRADE-OFF ANALYSES 18
TECHNICAL RISK AND OPPORTUNITY MANAGEMENT 18
TECHNICAL PERFORMANCE MEASURES AND METRICS 19
TECHNICAL REVIEWS 19
PDR 19
Critical Design Review (CDR) 19
CONFIGURATION MANAGEMENT 20
MODELING AND SIMULATION 20
MANUFACTURING AND PRODUCIBILITY 20
SOFTWARE 20
RELIABILITY AND MAINTAINABILITY (R&M) 21
MODULAR OPEN SYSTEMS APPROACH 21
CORROSION PREVENTION AND CONTROL 22
ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH (ESOH) 22
PESHE 22
NEPA/E.O. 12114 22
Mishap Investigation Support 23

INSENSITIVE MUNITIONS 23
ITEM UNIQUE IDENTIFICATION. 23
SPECTRUM SUPPORTABILITY 23
PROGRAM SUPPORT ASSESSMENTS (PSAs) 23

ENCLOSURE 4: DEVELOPMENTAL TEST AND EVALUATION (DT&E) 25
PURPOSE 25
OVERVIEW 25
T&E MANAGEMENT 26
DT&E ACTIVITIES 27
DT&E PLANNING CONSIDERATIONS 28
DT&E EXECUTION, EVALUATION, AND REPORTING 31
DT&E Execution 31
DASD(DT&E) Program Assessments 31
DT&E Reports and Data 31

ENCLOSURE 5: OPERATIONAL AND LIVE FIRE TEST AND EVALUATION (OT&E AND LFT&E) 33
OVERVIEW 33
APPLICABILITY 33
DOT&E OVERSIGHT LIST 34
T&E PROGRAM MANAGEMENT 34
Early Engagement 34
Lead Operational Test Agency (OTA) 35
Required Documentation 35
T&E PROGRAM PLANNING 35
OT&E ACTIVITIES 37
Operational Assessments (OAs) 37
RFPs 37
OT&E for Reliability and Maintainability 38
Use of Modeling and Simulation 38
OT&E FOR SOFTWARE 38
CYBERSECURITY 40
LFT&E 40
RESOURCES AND SCHEDULE 40
OPERATIONAL AND LIVE FIRE T&E EXECUTION 41
Planning Test Events 42
Conducting Test Events 44
Data Management, Evaluation, and Reporting 45
OPERATIONAL TEST READINESS 46
CERTIFICATIONS 46
TEMP EVOLUTION THROUGH THE ACQUISITION MILESTONES 46

ENCLOSURE 6: LIFE-CYCLE SUSTAINMENT 47

ENCLOSURE 7: HUMAN SYSTEMS INTEGRATION (HSI) 48
PURPOSE 48
GENERAL 48
HSI PLANNING 48
Human Factors Engineering 48
Personnel 48
Habitability 48
Manpower 49
Training 49
Safety and Occupational Health 49
Force Protection and Survivability 49

ENCLOSURE 8: AFFORDABILITY ANALYSIS AND INVESTMENT CONSTRAINTS 50

ENCLOSURE 9: ANALYSIS OF ALTERNATIVES (AOA) 51

ENCLOSURE 10: COST ESTIMATING AND REPORTING 52

ENCLOSURE 11: REQUIREMENTS APPLICABLE TO ALL PROGRAMS CONTAINING INFORMATION TECHNOLOGY (IT) 53

ENCLOSURE 12: URGENT CAPABILITY ACQUISITION 54

ENCLOSURE 13: CYBERSECURITY IN THE DEFENSE ACQUISITION SYSTEM 55
PROGRAM MANAGER RESPONSIBILITIES 55
Program Information 55
Organizations and Personnel 55
Enabling Networks 55
Systems, Enabling Systems, and Supporting Systems 55
ACTIVITIES TO MITIGATE CYBERSECURITY RISKS 55
Safeguard Program Information Against Cyber-Attack 56
Design for Cyber Threat Environments 56
Manage Cybersecurity Impacts to Information Types and System Interfaces to the DoDIN 58
PROTECTION PLANNING 58
Systems Engineering Plan (SEP) 58
PPP 58
TEMP 59
Risk Management Framework for DoD IT Security Plan and Cybersecurity Strategy 59
RESOURCES FOR EXECUTING CYBERSECURITY AND RELATED PROGRAM SECURITY ACTIVITIES 59

GLOSSARY 63

TABLES

1. Relationship of DoDI 5000.02T and New Policy 2
2. Cybersecurity and Related Program Security Resources and Publications 60

FIGURES

1. Operational or Major Live Fire Test Event: Planning, Approval, Execution, and Reporting 41

REFERENCES

(a) DoD Directive 5000.01, "The Defense Acquisition System," September 9, 2020
(b) Interim DoD Instruction 5000.02, "Operation of the Defense Acquisition System," November 26, 2013 (hereby cancelled)
(c) Office of Management and Budget Circular A-11, "Preparing, Submitting, and Executing the Budget," current edition
(d) Public Law 114-92, "National Defense Authorization Act for Fiscal Year 2016"
(e) Chairman of the Joint Chiefs of Staff Instruction 3170.01I, "Joint Capabilities Integration and Development System," January 23, 2015
(f) Assistant Secretary of Defense for Research and Engineering Guide, "Technology Readiness Assessment (TRA) Guidance," April 2011, as amended[1]
(g) Public Law 110-417, "The Duncan Hunter National Defense Authorization Act for Fiscal Year 2009," October 14, 2008
(h) Title 10, United States Code
(i) DoD Instruction 5000.74, "Defense Acquisition of Services," January 5, 2016
(j) Title 15, United States Code
(k) Public Law 109-364, "John Warner National Defense Authorization Act for Fiscal Year 2007," October 17, 2006
(l) Public Law 112-239, "National Defense Authorization Act for Fiscal Year 2013," January 2, 2013
(m) Public Law 111-383, "Ike Skelton National Defense Authorization Act for Fiscal Year 2011," January 7, 2011
(n) Public Law 101-576, "Chief Financial Officers Act of 1990," November 15, 1990
(o) Statement of Federal Financial Accounting Standards (SFFAS) No. 23, "Eliminating the Category National Defense Property, Plant, and Equipment," May 8, 2003
(p) Title 40, United States Code
(q) Public Law 106-398, "Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001," October 30, 2000
(r) Joint Capabilities Integration and Development System (JCIDS) Manual "Manual for the Operation of the Joint Capabilities Integration and Development System," current edition[2]
(s) Chairman of the Joint Chiefs of Staff Instruction 5123.01G, "Charter for Joint Requirements Oversight Council," February 12, 2015
(t) Defense Intelligence Agency Directive 5000.200, "Intelligence Threat Support for Major Defense Acquisition Programs," September 19, 2016[3]
(u) Defense Intelligence Agency Instruction 5000.002, "Intelligence Threat Support for Major Defense Acquisition Programs," September 19, 2016[4]
(v) Public Law 112-81, "National Defense Authorization Act for Fiscal Year 2012," December 31, 2011

[1] https://acc.dau.mil/CommunityBrowser.aspx?id=18545

[2] https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=1517681

[3] This is a controlled document. The office of primary responsibility is the Defense Intelligence Agency, (202) 231-0678

[4] This is a controlled document. The office of primary responsibility is the Defense Intelligence Agency, (202) 231-0678

(w) DoD Instruction 5000.73, "Cost Analysis Guidance and Procedures," March 13, 2020
(x) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(y) DoD Instruction 7041.03, "Economic Analysis for Decision-Making," September 9, 2015
(z) Public Law 102-538, "The National Telecommunications and Information Organization Act," October 27, 1992
(aa) Title 47, United States Code
(ab) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014
(ac) DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
(ad) DoD Instruction 8410.03, "Network Management (NM)," August 29, 2012, as amended
(ae) DoD Instruction 8320.04, "Item Unique Identification (IUID) Standards for Tangible Personal Property," September 3, 2015
(af) DoD Directive 5250.01, "Management of Intelligence Mission Data (IMD) in DoD Acquisition," January 22, 2013
(ag) Section 4321, Title 42, United States Code
(ah) Executive Order 12114, "Environmental Effects Abroad of Major Federal Actions," January 4, 1979
(ai) DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015
(aj) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, as amended
(ak) Federal Acquisition Regulation, current edition
(al) Defense Federal Acquisition Regulation Supplement, current edition
(am) DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009
(an) Public Law 111-23, "Weapon Systems Acquisition Reform Act of 2009," May 22, 2009
(ao) DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended[5]
(ap) DoD Instruction 4630.09, "Wireless Communications Waveform Development and Management," July 15, 2015
(aq) Public Law 109-163, "National Defense Authorization Act for Fiscal Year 2006," January 6, 2006
(ar) Memorandum of Agreement between the Director of National Intelligence and the Secretary of Defense concerning the Management of Acquisition Programs Executed at the Department of Defense Intelligence Community Elements, March 25, 2008[6]
(as) Intelligence Community Policy Guidance 801.1, "Acquisition," July 12, 2007[7]
(at) DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual," November 4, 2011
(au) American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) 748, March 2013

[5] This is a controlled document. The office of primary responsibility is Under Secretary of Defense (Intelligence), USDI.Pubs@osd.mil. Access requires a DoD PKI Certificate.
[6] www.fas.org/irp/dni/moa.pdf
[7] http://www.dni.gov/files/documents/ICPG/ICPG_801_1.pdf

(av) Data Item Management-81861, "Data Item Description: Integrated Program Management Report (IPMR)," June 20, 2012
(aw) Title 44, United States Code
(ax) DoD Instruction 5000.66, "Operation of the Defense Acquisition, Technology, and Logistics Workforce Education, Training, and Career Development Program," July 27, 2017
(ay) Under Secretary of Defense for Acquisition, Technology, and Logistics Policy Memorandum, "Key Leadership Positions and Qualification Criteria," November 8, 2013
(az) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014
(ba) DoD Instruction 2010.06, "Materiel Interoperability and Standardization with Allies and Coalition Partners," July 29, 2009
(bb) Defense Security Cooperation Agency Manual, "Security Assistance Management Manual (SAMM)," current version[8]
(bc) DoD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007
(bd) Military-Standard 882E, "DoD Standard Practice for System Safety," May 11, 2012
(bf) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, as amended
(bg) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended
(bh) DoD Instruction 5000.61, "DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)," December 9, 2009
(bi) DoD Instruction 4151.22, "Condition Based Maintenance Plus (CBM+) for Materiel Maintenance," October 16, 2012
(bj) Public Law 113-66, "National Defense Authorization Act for Fiscal Year 2014," December 26, 2013
(bk) DoD Manual 4160.28, Volume 1, "Defense Demilitarization: Program Administration," June 7, 2011
(bl) DoD Instruction 5000.67, "Prevention and Mitigation of Corrosion on DoD Military Equipment and Infrastructure," February 1, 2010
(bm) DoD Instruction 1100.22, "Policy and Procedures for Determining Workforce Mix," April 12, 2010
(bn) DoD Instruction 7041.04, "Estimating and Comparing the Full Costs of Civilian and Active Duty Military Manpower and Contract Support," July 3, 2013
(bo) DoD Directive 1322.18, "Military Training," January 13, 2009, as amended
(bp) DoD Directive 5105.84, "Director of Cost Assessment and Program Evaluation (DCAPE)," May 11, 2012
(bq) Office of the Secretary of Defense, Cost Assessment and Program Evaluation, "Operating and Support Cost-Estimating Guide," March 2014
(br) Global Information Grid (GIG) Technical Guidance Federation (GTGF)[9]
(bt) Office of Management and Budget Memorandum M-04-08, "Maximizing Use of SmartBuy and Avoiding Duplication of Agency Activities with the President's 24 E-Gov Initiatives," February 25, 2004

[8] http://www.samm.dsca.mil/
[9] http://www.disa.mil/Services/Enterprise-Engineering/IT-Standards

(bu) Office of Management and Budget Memorandum M-04-16, "Software Acquisition," July 1, 2004

(bv) Office of Management and Budget Memorandum M-05-25, "SmartBUY Agreement with Oracle," August 25, 2005

(bw) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014

(bx) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

(by) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015

(bz) DoD Instruction 3200.12, "DoD Scientific and Technical Information Program (STIP)," August 22, 2013

(ca) Section 794d of Title 29, United States Code

(cb) DoD Manual 8400.01-M, "Procedures for Ensuring the Accessibility of Electronic and Information Technology (E&IT) Procured by DoD Organizations," June 3, 2011

(cc) DoD Directive 5000.71, "Rapid Fulfillment of Combatant Commander Urgent Operational Needs," August 24, 2012

(cd) Public Law 107-314, "Bob Stump National Defense Authorization Act for Fiscal Year 2003," December 2, 2002

(ce) Defense Acquisition University Website[10]

(cf) Defense Acquisition University Glossary[11]

(cg) Public Law 113-291, "Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015," December 19, 2014

(ch) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Change to Major Defense Acquisition Program Milestone A Requirements," January 31, 2016[12]

(ci) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Change to Major Defense Acquisition Program Milestone B Requirements," January 31, 2016[13]

(cj) Integrated Program Management Report Implementation Guide, February 5, 2016[14]

(ck) DoD Instruction 4140.67, "DoD Counterfeit Prevention Policy," April 26, 2013

(cl) Directive Type Memo 17-001, "Cybersecurity in the Defense Acquisition System," January 11, 2017 (hereby cancelled)

(cm) DoD Directive 5135.02, "Under Secretary of Defense for Acquisition and Sustainment (USD(A&S))," July 15, 2020

(cn) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012

(co) DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010

(cp) Part 236 of Title 32, Code of Federal Regulations

(cq) Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," February 13, 2015

[10] http://www.dau.mil/default.aspx

[11] https://dap.dau.mil/glossary/Pages/Default.aspx

[12] https://ebiz.acq.osd.mil/DABCalendar/Home/Document/31 (access requires Common Access Card (CAC))

[13] https://ebiz.acq.osd.mil/DABCalendar/Home/Document/32 (access requires CAC)

[14] http://www.acq.osd.mil/evm/docs/IPMR%20Implementation%20Guide.pdf

(cr) Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation, “Department of Defense Cybersecurity Test and Evaluation Guidebook,” July 1, 2015

(cs) Director, Operational Test and Evaluation, “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs,” August 1, 2014

(ct) Office of the Deputy Assistant Secretary of Defense for Systems Engineering, “Guidance to Stakeholders for Implementing Defense Federal Acquisition Supplement Clause 252.204-7012,” August 2015

(cu) DoD Instruction 8530.01, “Cybersecurity Activities Support to DoD Information Network Operations,” March 7, 2016

(cv) Office of the Deputy Assistant Secretary of Defense for Systems Engineering, “Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs,” June 2015

(cw) DoD Instruction 5000.75, “Business Systems Requirements and Acquisition,” February 2, 2017

(cx) Deputy Secretary of Defense Memorandum, “Establishment of the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment,” July 13, 2018

(cy) DoD Instruction 5010.44, “Intellectual Property (IP) Acquisition and Licensing,” October 16, 2019

(cz) DoD Instruction 5025.01, “DoD Issuances Program,” August 1. 2016, as amended

(da) DoD Instruction 5000.82, “Acquisition of Information Technology (IT),” April 21, 2020

(db) DoD Instruction 5000.83, “Technology and Program Protection to Maintain Technological Advantage,” July 20, 2020

(dc) DoD Instruction 5000.85, “Major Capability Acquisition,” August 6, 2020

(de) DoD Instruction 5000.81, “Urgent Capability Acquisition,” December 31, 2019

ENCLOSURE 1

ACQUISITION PROGRAM CATEGORIES AND COMPLIANCE REQUIREMENTS

Enclosure 1 was removed through formal coordination and approval of Reference (dc); necessary information can be found in that issuance.

ENCLOSURE 2

PROGRAM MANAGEMENT

Enclosure 2 was removed through formal coordination and approval of Reference (dc); necessary information can be found in that issuance.

ENCLOSURE 3

SYSTEMS ENGINEERING

1. PURPOSE. This enclosure describes the policies and procedures regarding the application of systems engineering to defense acquisition. Systems engineering provides the integrating technical processes and design leadership to define and balance system performance, life-cycle cost, schedule, risk, and system security within and across individual systems and programs. The Program Manager, with support from the Lead Systems Engineer, will embed systems engineering in program planning and execution to support the entire system life cycle.

2. SYSTEMS ENGINEERING PLAN

a. Program Managers will prepare a Systems Engineering Plan (SEP) as a management tool to guide the systems engineering activities on the program. The SEP will be submitted to the MDA for approval before each milestone review, beginning with Milestone A. At each milestone and at the Development RFP Release Decision Point, the SEP will support the acquisition strategy, including the program interdependencies, and communicate the overall technical approach to balance system performance, life-cycle cost, and risk in addressing warfighter needs. The SEP will describe the program's overall technical approach, including key technical risks, processes, resources, organization, metrics, and design considerations. It will also detail the timing and criteria for the conduct of technical reviews. The use of mandatory tables in the SEP is intended to support more detailed technical planning during the system life cycle in order to provide effective management and control of the program's technical progress and the execution of risk mitigation activities. The SEP will address system integration with existing and approved architectures and capabilities. Program managers will identify and manage risk of external dependencies which are outside their span of control in order to ensure timely design, development, deployment, and sustainment of the system. Program managers will document interface requirements and interface products to track interdependent program touch points. The technical planning documented in the SEP will guide the details in the program's schedule. Program managers should include the SEP (either an approved Plan or a draft Plan) in the RFP as either guidance or a compliance document depending on the maturity of the plan and the acquisition strategy.

b. The Deputy Assistant Secretary of Defense (Systems Engineering) (DASD(SE)) will review the SEP for all Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs.

(1) DoD Components will submit the SEPs to the DASD(SE) at least 45 calendar days before the scheduled DAB milestone review.

(2) For Milestone B, the DoD Component-approved draft SEP will be provided to the DASD(SE) 45 calendar days prior to the Development RFP Release Decision Point. If continuing engineering activities such as the Preliminary Design Review (PDR) create the need

for substantive changes to the SEP, it will be revised and resubmitted for review before Milestone B. Program managers will update the SEP as needed after contract award to reflect any changes due to the contractor's technical approach and details not available prior to contract award. The updated SEP will be provided to the DASD(SE).

3. DEVELOPMENT PLANNING. The decisions to enter into the acquisition process, to mature technologies, and to begin system design must be based on early systems engineering analysis and assessments and a strong technical foundation.

a. In preparation for the Materiel Development Decision, and to inform an Analysis of Alternatives (AoA), the DoD Components will conduct early systems engineering analyses and conduct an assessment of how the proposed candidate materiel solution approaches are technically feasible and have the potential to effectively address capability gaps, desired operational attributes, and associated external dependencies.

b. During the Materiel Solution Analysis Phase, the Components will conduct early systems engineering analyses, informed by and in support of the AoA, to support selection of a preferred materiel solution and development of the draft Capability Development Document (or equivalent requirements document).

c. In preparation for Milestone A, and to provide the technical basis for executing the Technology Maturation and Risk Reduction Phase, the Program Manager will conduct an early systems engineering assessment of technical risks and develop the technical approach for acquiring the product. This technical assessment will include software, integration, manufacturing, and reliability risks. The results will be incorporated in the SEP for Milestone A.

4. SYSTEMS ENGINEERING TRADE-OFF ANALYSES

a. During the acquisition life cycle, the Program Manager will conduct systems engineering trade-off analyses to assess system affordability and technical feasibility to support requirements, investment, and acquisition decisions. Systems engineering trade-off analyses will depict the relationships between system life-cycle cost and the system's performance requirements, design parameters, and delivery schedules. The analysis results should be reassessed over the life cycle as system requirements, design, manufacturing, test, and logistics activities evolve and mature.

b. In support of the validation of the Capability Development Document (or equivalent requirements document), the Program Manager will conduct a systems engineering trade-off analysis showing how cost varies as a function of system requirements (including KPPs), major design parameters, and schedule. The results will be provided to the MDA and will identify major affordability drivers and show how the program meets affordability constraints.

5. TECHNICAL RISK AND OPPORTUNITY MANAGEMENT. Technical risk management should address risk identification, analysis, mitigation planning, mitigation implementation, and

tracking. Technical risks should be quantified and implications reflected in the program's Integrated Master Schedule and Integrated Master Plan. The Program Manager should also work with the applicable science and technology communities and Component acquisition leadership to influence technology investment planning. The goal is to both mitigate risks and create opportunities for technology development outcomes that could have a positive impact on meeting performance objectives as well as thresholds. Program risks, and opportunities as applicable, will be assessed at technical reviews and will include specific cost and schedule implications.

6. TECHNICAL PERFORMANCE MEASURES AND METRICS. The Program Manager will use technical performance measures and metrics to assess program progress. Analysis of technical performance measures and metrics, in terms of progress against established plans, will provide insight into the technical progress and risk of a program.

7. TECHNICAL REVIEWS. Program Managers will:

a. Conduct technical reviews of program progress for systems in development as a basis for transitioning between phases within the development plan of work. Reviews will be event-driven and based on the review entrance criteria as documented in the SEP.

b. Program Managers will plan for and conduct design reviews as needed to manage program planning and execution. Design review planning will be included in the SEP. Any program that is not initiated at Milestone C will include the following design reviews:

(1) PDR. The PDR assesses the maturity of the preliminary design supported by the results of requirements trades, prototyping, and critical technology demonstrations. The PDR will establish the allocated baseline and confirm that the system under review is ready to proceed into detailed design (development of build-to drawings, software code-to documentation, and other fabrication documentation) with acceptable risk. For MDAPs and MAIS programs, a system-level PDR assessment will be conducted and provided to the MDA. For Acquisition Category (ACAT) ID and ACAT IAM programs, DASD(SE) will conduct the PDR assessment to inform the MDA of technical risks and the program's readiness to proceed into detailed design. The Program Manager will make the program information needed for this assessment available and provide for DASD(SE) participation in the program's PDR process. For ACAT IC and ACAT IAC programs, the Component Acquisition Executive (CAE) will conduct the PDR assessment.

(2) Critical Design Review (CDR). The CDR assesses design maturity, design build-to or code-to documentation, and remaining risks and establishes the initial product baseline. It will be used as the decision point that the system design is ready to begin developmental prototype hardware fabrication or software coding with acceptable risk. For MDAPs and MAIS programs, a system-level CDR assessment will be conducted and the results will be provided to the MDA. For ACAT ID and IAM programs, DASD(SE) will conduct the CDR assessment to inform the MDA of the program's design maturity, technical risks, and the program's readiness to begin

developmental prototype hardware fabrication and/or software coding with acceptable risk. As the basis for preparation of a CDR assessment, the Program Manager will provide for DASD(SE) participation in the program's CDRs and the Program Manager will make needed program artifacts and information available. For ACAT IC and IAC programs, the CAE will conduct the CDR assessment.

8. CONFIGURATION MANAGEMENT. The Program Manager will use a configuration management approach to establish and control product attributes and the technical baseline across the total system life cycle. This approach will identify, document, audit, and control the functional and physical characteristics of the system design; track any changes; provide an audit trail of program design decisions and design modifications; be integrated with the SEP and technical planning; and be consistent with the IP Strategy. At completion of the system level CDR, the Program Manager will assume control of the initial product baseline, to the extent that the competitive environment permits.

9. MODELING AND SIMULATION. The Program Manager will integrate modeling and simulation activities into program planning and engineering efforts. These activities will support consistent analyses and decisions throughout the program's life cycle. Models, data, and artifacts will be integrated, managed, and controlled to ensure that the products maintain consistency with the system and external program dependencies, provide a comprehensive view of the program, and increase efficiency and confidence throughout the program's life cycle.

10. MANUFACTURING AND PRODUCIBILITY. The Program Manager will ensure manufacturing and producibility risks are identified and managed throughout the program's life cycle. Beginning in the Materiel Solution Analysis Phase, manufacturing readiness and risk will be assessed and documented in the SEP. By the end of the Technology Maturation and Risk Reduction Phase, manufacturing processes will be assessed and demonstrated to the extent needed to verify that risk has been reduced to an acceptable level. During the Engineering and Manufacturing Development Phase, Program Managers will assess the maturity of critical manufacturing processes to ensure they are affordable and executable. Prior to a production decision, the Program Manager will ensure manufacturing and producibility risks are acceptable, supplier qualifications are completed, and any applicable manufacturing processes are or will be under statistical process control.

11. SOFTWARE. The development and sustainment of software can be a major portion of the total system life-cycle cost and should be considered at every decision point in the acquisition life cycle. A phased software development approach using testable software builds and/or fieldable software increments enables the developers to deliver capability in a series of manageable, intermediate products to gain user acceptance and feedback for the next build or increment, and reduce the overall level of risk. The SEP should address the following: software unique risks; inclusion of software in technical reviews; identification, tracking, and reporting of

metrics for software technical performance, process, progress, and quality; software safety and security considerations; and software development resources.

12. RELIABILITY AND MAINTAINABILITY (R&M)

a. The Program Manager will formulate a comprehensive R&M program using an appropriate strategy to ensure reliability and maintainability requirements are achieved. The program will consist of engineering activities including for example: R&M allocations, block diagrams and predictions; failure definitions and scoring criteria; failure mode, effects and criticality analysis; maintainability and built-in test demonstrations; reliability testing at the system and subsystem level; and a failure reporting, analysis, and corrective action system maintained through design, development, production, and sustainment. The R&M program is an integral part of the systems engineering process.

b. For MDAPs, the Program Manager will prepare a preliminary Reliability, Availability, Maintainability and Cost Rationale (RAM-C) Report in support of the Milestone A decision. This report provides a quantitative basis for reliability requirements, and improves cost estimates and program planning. This report will be attached to the SEP at Milestone A, and updated in support of the Development RFP Release Decision Point, Milestone B, and Milestone C.

c. Reliability growth curves (RGCs) will reflect the reliability growth strategy and be employed to plan, illustrate, and report reliability growth. RGCs will be included in the SEP at Milestone A and updated in the draft SEP submitted at the Development RFP Release Decision Point and in the final approved SEP and Test and Evaluation Master Plan submitted at Milestone B. RGCs will be stated in a series of intermediate goals and tracked through fully integrated, system-level test and evaluation events at least until the reliability threshold is achieved. If a single curve is not adequate to describe overall system reliability, curves for critical subsystems should also be employed.

d. Program offices, developmental test agencies, and operational test agencies will assess the reliability growth required for the system to achieve its reliability threshold during testing, and report the results of those assessments to the acquisition chain of command including the MDA.

e. Reliability growth will be monitored and reported throughout the acquisition process. Program managers will report the status of R&M objectives and/or thresholds as part of the formal design review process, and during systems engineering technical reviews or other reviews. RGCs will be employed to report reliability growth status at Defense Acquisition Executive Summary reviews.

13. MODULAR OPEN SYSTEMS APPROACH. Program Managers, with support from the Lead Systems Engineer, are responsible for applying modular approaches in product designs where feasible and cost-effective. They are also responsible for acquiring data and IP that are both appropriate (10 U.S.C. 2320 (Reference (h)) and essential to achieving the expected benefits (see Reference (dc) for additional information on MOSA and IP). Modular designs coupled with

an appropriately open business model provide a valuable mechanism for continuing competition and incremental upgrades, and to facilitate reuse across the joint force.

14. CORROSION PREVENTION AND CONTROL. The Program Manager will identify and evaluate corrosion considerations throughout the acquisition and sustainment phases that reduce, control, or mitigate corrosion in sustainment. The Program Manager will perform corrosion prevention and control planning and include corrosion control management and design considerations for corrosion prevention and control in the SEP and Life-Cycle Sustainment Plan. The Program Manager will ensure that corrosion control requirements are included in the design and verified as part of test and acceptance programs.

15. ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH (ESOH). The Program Manager will integrate ESOH risk management into the overall systems engineering process for all engineering activities throughout the system's life cycle. As part of risk reduction, the Program Manager will eliminate ESOH hazards where possible, and manage ESOH risks where hazards cannot be eliminated. The Program Manager will use the methodology in MIL-STD-882E (Reference (bd)). Program Managers will assess the status of ESOH risks and acceptance decisions at technical reviews. Acquisition program reviews and fielding decisions will address the status of all high and serious risks. Prior to exposing people, equipment, or the environment to known system-related ESOH hazards, the Program Manager will document that the associated risks have been accepted by the following acceptance authorities: the CAE for high risks, PEO-level for serious risks, and the Program Manager for medium and low risks. The user representative, as defined in MIL-STD-882E, must be part of this process throughout the life cycle and will provide formal concurrence prior to all serious- and high-risk acceptance decisions. For joint programs, the ESOH risk acceptance authorities reside within the lead DoD Component. Program managers will document the ESOH planning in the SEP and will document the results of the planning implementation in the Programmatic ESOH Evaluation (PESHE) and the compliance schedule required by the National Environmental Policy Act (NEPA) (Reference (ag)) and Executive Order (E.O.) 12114 (Reference (ah)) (NEPA/E.O. 12114).

a. PESHE. The Program Manager, regardless of ACAT level, will prepare and maintain a PESHE to document data generated by ESOH analyses conducted in support of program execution. The PESHE will include at a minimum identification of ESOH risks and their status; and, identification of hazardous materials, wastes, and pollutants (discharges/emissions/noise) associated with the system and its support as well as the plans for minimization and/or safe disposal.

b. NEPA/E.O. 12114. The Program Manager will prepare and maintain a NEPA/E.O. 12114 Compliance Schedule that covers all known or projected system-related activities that may trigger compliance requirements including testing, fielding, and support of the system. The Compliance Schedule will incorporate the test schedules and locations identified in the Test and Evaluation Master Plan to enable consideration of potential impacts to the environment and completion of appropriate documentation in accordance with DoD Component implementing procedures. The Program Manager will conduct and document the NEPA/E.O. 12114 analyses for which the Program Manager is the action proponent, and provide system-specific analyses and data to support other organizations' NEPA/E.O. 12114 analyses of system-related activities for which the Program Manager is not the proponent. The CAE (for joint programs, the CAE of the lead DoD Component) or designee, is the approval authority for system-related NEPA/E.O. 12114 documentation for which the Program Manager is the proponent.

c. Mishap Investigation Support. The Program Manager will support system-related Class A and B mishap investigations by providing analyses of hazards that contributed to the mishap and recommendations for materiel risk mitigation measures, especially those that minimize human errors, as required by 10 U.S.C. 2255 (Reference (h)).

16. INSENSITIVE MUNITIONS. For all systems containing energetics, the Program Manager will comply with Insensitive Munitions requirements in accordance with the DoD and Component policy requirements (as required by 10 U.S.C. 2389 (Reference (h)).

17. ITEM UNIQUE IDENTIFICATION. The Program Manager will plan for and implement item unique identification to identify and track applicable major end items, configuration-controlled items, and government-furnished property to enhance life-cycle management of assets in systems acquisition and sustainment, and to provide more accurate asset valuation and property accountability. Item unique identification planning and implementation will be documented in an Item Unique Identification Implementation Plan linked to the program's SEP. DoD Instruction 8320.04 (Reference (ae)) provides the standards for unique item identifiers.

18. SPECTRUM SUPPORTABILITY. Program managers are responsible for ensuring compliance of their programs with U.S. and host nation electromagnetic spectrum regulations, in accordance with 47 U.S.C. section 305 and sections 901 through 904 (Reference (aa)) and section 104 of P.L.102-538 (Reference (z)). Program managers will also submit written determinations to the Component Chief Information Officer (CIO) or equivalent that the electromagnetic spectrum necessary to support the operation of the system during its expected life cycle is or will be available in accordance with DoD Instruction 4650.01 (Reference (am)). These determinations will be the basis for recommendations provided to the MDA by the Component CIO or equivalent.

19. PROGRAM SUPPORT ASSESSMENTS (PSAs). The Office of the DASD(SE) will conduct independent, cross-functional PSAs of MDAPs' and MAIS programs, and other program's as directed by the DAE, to assess technical management and systems engineering progress and plans. PSAs are for the purpose of assisting program managers' technical planning, and to improve execution by sharing best practices and lessons learned from other programs. The DASD(SE) will advise technical authorities on the incorporation of best practices for systems engineering from across the DoD. Risk identification and risk mitigation assistance will be one focus of the PSAs. These reviews may also support acquisition milestones, decision

reviews, or be conducted in response to technical issues on ACAT ID and IAM programs. These assessments are intended to help program managers shape their programs' technical planning and improve execution by providing actionable recommendations and identifying engineering and integration risks, as well as potential mitigation activities. The DoD Components will provide access to all program records and data including technical review artifacts and classified, unclassified, competition sensitive, and proprietary information that the DASD(SE) considers necessary to carry out these assessments in accordance with 10 U.S.C. 139b (Reference (h)).

ENCLOSURE 4

DEVELOPMENTAL TEST AND EVALUATION (DT&E)

1. PURPOSE. This enclosure provides policy and procedure for developmental test and evaluation of defense acquisition programs.

2. OVERVIEW

a. Program managers use DT&E activities to manage and mitigate risks during development, to verify that products are compliant with contractual and operational requirements, and to inform decision makers throughout the program life cycle. DT&E provides program engineers and decision makers with knowledge to measure progress, identify problems, and to characterize system capabilities and limitations, and manage technical and programmatic risks. DT&E results are also used as exit criteria to ensure adequate progress prior to investment commitments or initiation of phases of the program, and as the basis for contract incentives.

b. DT&E starts with capability requirements and continues through product development, delivery, and acceptance; transition to operational test and evaluation (T&E); production; and operations and support. Consideration of developmental test and evaluation in the requirements and systems engineering processes ensures that capability requirements are measurable, testable, and achievable. Identifying and correcting deficiencies early is less costly than discovering system deficiencies late in the acquisition process.

c. The Program Manager will use a Test and Evaluation Master Plan (TEMP) as the primary planning and management tool for the integrated test program. Whenever feasible, testing will be conducted in an integrated fashion to permit all stakeholders to use data in support of their respective functions. Integrated testing requires the collaborative planning and collaborative execution of test phases and events to provide shared data in support of independent analysis, evaluation, and reporting by all stakeholders, particularly the systems engineering, developmental (both contractor and government) and operational T&E communities. The Program Manager will establish an integrated test planning group consisting of empowered representatives of test data producers and consumers (to include all applicable stakeholders) to ensure collaboration and to develop a strategy for robust, efficient testing to support systems engineering, evaluations, and certifications throughout the acquisition life cycle.

d. The Program Manager will identify the test resources needed to execute the DT&E program to acquire the data that will be used to understand program progress, identify issues, verify compliance, and balance cost and performance. Test resource requirements will be included in the TEMP.

e. The Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)) will monitor the development test and evaluation program activities of Major Defense Acquisition Programs (MDAPs) and review the DT&E plans for those programs in the

TEMP. The DASD(DT&E) will provide a recommendation to approve or disapprove the MDAP DT&E plans as well as advise the relevant technical authorities for these programs on the incorporation of best practices for developmental test from across the Department. For ACAT IA, and ACAT II and below programs, the Component Acquisition Executive will designate a DT&E organization to monitor DT&E activities and recommend approval or disapproval of the DT&E plans in the TEMP. For all programs, the MDA (or designee) will approve or disapprove the DT&E plans in the TEMP. DASD(DT&E) authorities, responsibilities, and functions are described in 10 U.S.C. 139b (Reference (h)).

3. T&E MANAGEMENT

a. Program managers for MDAPs and MAIS programs will designate a Chief Developmental Tester in accordance with 10 U.S.C. 139b and 1706 (Reference (h)). The Chief Developmental Tester will be responsible for coordinating the planning, management, and oversight of all DT&E activities; maintaining insight into contractor activities; overseeing the T&E activities of other participating government activities; and helping the Program Manager make technically informed, objective judgments about contractor and government T&E planning and results. The Chief Developmental Tester will chair the integrated test planning group.

b. Program managers for MDAPs will designate a government test agency to serve as the lead DT&E organization in accordance with 10 U.S.C. 139b. The lead DT&E organization will be responsible for providing technical expertise on T&E issues to the Chief Developmental Tester; conducting DT&E activities as directed by the Chief Developmental Tester or his or her designee; supporting certification and accreditation activities when feasible; assisting the Chief Developmental Tester in providing oversight of contractors; and assisting the Chief Developmental Tester in reaching technically informed, objective judgments about contractor and government T&E planning and results. For all other programs, a lead DT&E organization should be used, when feasible, and identified in the TEMP.

c. The designation of a Chief Developmental Tester and lead DT&E organization will be made as soon as practicable after the program office is established.

d. The Program Manager will use the TEMP as the primary planning and management tool for all test activities starting at Milestone A. The Program Manager will prepare and update the TEMP as needed and to support acquisition milestones or decision points. For the Full-Rate Production Decision Review or the Full Deployment Decision and thereafter, the MDA may require TEMP updates or addendums to plan for additional testing. Section 5 in Enclosure 5 of this instruction has additional policy for the TEMP in the context of operational testing.

e. Program managers for programs under DASD(DT&E) oversight will designate a T&E Working-level Integrated Product Team (WIPT) (also known as an Integrated Test Team), as soon as practicable after the Materiel Development Decision. The T&E WIPT develops and tracks the T&E program in all phases. The T&E WIPT will include empowered representatives of test data stakeholders such as Systems Engineering, DT&E, Operational T&E, Live Fire T&E, Product Support, the user, the intelligence community, and applicable certification authorities.

f. The Program Manager will take full advantage of DoD ranges, labs, and other resources. Systems have become more complex and resource constraints often force tradeoffs in the type and scope of testing that can be performed. The DT&E budget and schedule must allow testing that adequately verifies performance to contractual requirements in a controlled environment and to operational requirements.

4. DT&E ACTIVITIES

a. DT&E activities will start when requirements are being developed to ensure that key technical requirements are measurable, testable, and achievable.

b. A robust DT&E program includes a number of key activities to provide the data and assessments for decision making. The DT&E program will:

(1) Verify achievement of critical technical parameters and the ability to achieve KPPs, and assess progress toward achievement of critical operational issues.

(2) Assess the system’s ability to achieve the thresholds prescribed in the capabilities documents.

(3) Provide data to the Program Manager to enable root cause determination and to identify corrective actions.

(4) Validate system functionality.

(5) Provide information for cost, performance, and schedule tradeoffs.

(6) Assess system specification compliance.

(7) Report on program progress to plan for reliability growth and to assess reliability and maintainability performance for use during key reviews.

(8) Identify system capabilities, limitations, and deficiencies.

(9) Include T&E activities to detect cyber vulnerabilities within custom and commodity hardware and software.

(10) Assess system safety.

(11) Assess compatibility with legacy systems.

(12) Stress the system within the intended operationally relevant mission environment.

(13) Support cybersecurity assessments and authorization, including Risk Management Framework security controls.

(14) Support the interoperability certification process.

(15) Document achievement of contractual technical performance, and verify incremental improvements and system corrective actions.

(16) Assess entry criteria for Initial Operational Test and Evaluation (IOT&E) and Follow-On Operational Test and Evaluation.

(17) Provide DT&E data to validate parameters in models and simulations.

(18) Assess the maturity of the chosen integrated technologies.

5. DT&E PLANNING CONSIDERATIONS

a. The Program Manager will:

(1) Use the TEMP as the primary test planning and management document.

(2) The TEMP will:

(a) Contain an integrated test program summary and master schedule of all major test events or test phases.

(b) Include an event-driven testing schedule that will allow adequate time to support pre-test predictions; testing; post-test analysis, evaluation, and reporting; reconciliation of predictive models; and adequate time to support execution of corrective actions in response to discovered deficiencies. The schedule should allow sufficient time between DT&E and IOT&E for rework, reports, and analysis and developmental testing of critical design changes.

(c) Be a source document when developing the RFP.

(d) Guide how contractor proposals will address program test needs such as: test articles; T&E data rights; government access to the Failure Reporting, Analysis and Corrective Action System and other test outcome repositories; built-in test and embedded instrumentation data (including software log files); contractor verification requirements; government use of contractor-conducted T&E; government review and approval of contractor T&E plans; government witness of contractor test events; and government review of contractor evaluations. See section 5 in Enclosure 5 of this instruction for additional details.

(e) Include identification of all contractor and government system level reliability testing needed to support initial reliability planning estimates. The Program Manager will include the reliability developmental evaluation methodology for reliability critical items. The military departments/program managers will collect and retain data from the T&E of the reliability and maintainability of major weapon systems to inform system design decisions, provide insight into sustainment costs, and inform estimates of operating and support costs for such systems.

(f) Starting at Milestone B, include one or more reliability growth curves (RGCs).

1. If a single curve is not adequate to describe the overall system reliability, curves for critical subsystems with rationale for their selection will be provided.

2. For software (in any system), the TEMP will include projected and observed software maturity metrics. For hardware acquisitions, Milestone B RGCs will consist of observed (when available) and projected reliability.

3. RGCs will be stated in a series of intermediate goals tracked through fully integrated, system-level T&E events until the reliability threshold is achieved.

(3) Use scientific test and analysis techniques to design an effective and efficient test program that will produce the required data to characterize system behavior across an appropriately selected set of factors and conditions.

(4) Identify each developmental test phase or major developmental test event as a contractor or government DT&E. All programs will plan for the conduct of DT&E and/or integrated testing to provide confidence in the system design solution. Each major developmental test phase or event (including Test Readiness Reviews) will have test entrance and exit criteria. The developmental test completion criteria (customer needs) will dictate what data are required from the test event.

(5) Ensure that all test infrastructure and/or tools (e.g., models, simulations, automated tools, synthetic environments) to support acquisition decisions will be verified, validated, and accredited (VV&A) by the intended user or appropriate agency. Test infrastructure, tools, and/or the VV&A strategy including the VV&A authority for each tool or test infrastructure asset will be documented in the TEMP. Program Managers will plan for the application and accreditation of any modeling and simulation tools supporting DT&E.

(6) Develop complete resource estimates for T&E to include: test articles, test sites and instrumentation, test support equipment, threat representations and simulations, test targets and expendables, support for operational forces used in test (both friendly and threat), models and simulations, testbeds, joint mission environment, distributed test networks, funding, manpower and personnel, training, federal/state/local requirements, range requirements, and any special requirements (e.g., explosive ordnance disposal requirements or corrosion prevention and control). Resources will reflect the best estimate for conducting all test activities. Resources will be mapped against the developmental evaluation framework and schedule to ensure adequacy and availability.

(7) Ensure that resource estimates identified in the TEMP are matched against the schedule and justified by analysis.

(8) Resource and ensure threat-appropriate Red Team/Penetration testing to emulate the threat of hostile penetration of program information systems in the operational environment. Additional guidance on Red Team operations is included in Chairman of the Joint Chiefs of Staff Instruction 6510.01F (Reference (bf)).

(9) Develop a strategy and budget resources for cybersecurity testing. The test program will include, as much as possible, activities to test and evaluate a system in a mission environment with a representative cyber-threat capability.

(10) Ensure that each major developmental test phase or event in the planned test program has a well-defined description of the event, specific objectives, scope, appropriate use of modeling and simulation, and a developmental evaluation methodology.

(11) Describe a developmental evaluation methodology in the TEMP starting at Milestone A that will provide essential information on programmatic and technical risks as well as information for major programmatic decisions. Starting at Milestone B, the developmental evaluation methodology will include a developmental evaluation framework to identify key data that will contribute to assessing progress toward achieving: KPPs, critical technical parameters, key system attributes, interoperability requirements, cybersecurity requirements, reliability growth, maintainability attributes, developmental test objectives, and others as needed. In addition, the developmental evaluation framework will show the correlation and mapping between test events, key resources, and the decision supported. The developmental evaluation methodology will support a Milestone B assessment of planning, schedule, and resources and a Milestone C assessment of performance, reliability, interoperability, and cybersecurity.

(12) Develop a software test automation strategy to include when key test automation software components or services will be acquired and how those decisions will be made.

b. Programs will use government T&E capabilities unless an exception can be justified as cost-effective to the government. Program managers will conduct a cost-benefit analysis for exceptions to this policy and obtain approval through the TEMP approval process before acquiring or using non-government, program unique test facilities or resources.

c. In accordance with DoD Instruction 8510.01 (Reference (bg)), all programs must have security controls implemented consistent with their information and system categorization. Program managers will ensure appropriate testing to evaluate capability to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The Defense Intelligence Agency (DIA), in coordination with the Program Manager, will determine the generation of the relevant operational threat environment based on the Validated On-line Life-cycle Threat Report, the Multi-Service Force Deployment, the Joint Country Forces Assessment and scenario support products in accordance with DIA Directive 5000.200 (Reference (t)) and DIA Instruction 5000.002 (Reference (u)).

d. Systems that operate as part of a system of systems may require deployment of additional test assets to evaluate end-to-end capabilities. Program managers will ensure that adequate testing of total system of systems performance is conducted as part of the DT&E program.

e. For accelerated acquisition and urgent need programs, the levels of developmental testing required will be highly tailored to emphasize schedule over other considerations. Required testing to verify safety, capabilities, and limitations will be performed consistent with the urgency of fielding the capability. Responsibility for determining developmental testing requirements will be delegated to the lowest practical level. Urgent need programs will generally not be on an OSD DT&E Engagement list. If an Accelerated Acquisition program is on the DT&E Engagement list, complete developmental testing may be deferred so as not to impede early fielding; however, an operational assessment will typically be conducted. See paragraph 6a in Enclosure 5 of this instruction for a discussion of operational assessments, and Reference (de) for the policy and procedure regarding acquisition programs that respond to urgent needs.

6. DT&E EXECUTION, EVALUATION, AND REPORTING

a. DT&E Execution. As the Program Manager executes the program's strategy for the DT&E, the Program Manager and test team will develop detailed test plans for each developmental test event identified in the TEMP. Test plans must consider the potential impacts on personnel and the environment in accordance with 10 U.S.C. 4321-4347 (Reference (ag)) and Executive Order 12114 (Reference (ah)). The Program Manager, in concert with the user and T&E community, will provide safety releases (to include National Environmental Policy Act documentation, safety, and occupational health risk acceptance in accordance with section 16 in Enclosure 3 of this instruction) to testers prior to any test that may impact safety of personnel. A Test Readiness Review will be conducted for those events identified in the TEMP.

b. DASD(DT&E) Program Assessments. For MDAPs, MAIS programs, and USD(AT&L)-designated special interest programs, the DASD(DT&E) will provide the MDA with a program assessment at the Development RFP Release Decision Point, Milestones B and C, and updated to support the Operational Test Readiness Review or as requested by the MDA or Program Manager. The program assessment will be based on the completed DT&E and any Operational T&E activities completed to date, and will address the adequacy of the program planning, the implications of testing results to date, and the risks to successfully meeting the goals of the remaining T&E events in the program.

c. DT&E Reports and Data

(1) The DASD(DT&E) and the acquisition chain of command (including the Program Manager) and their designated representatives will have full and prompt access to all ongoing developmental testing, and all developmental test records and reports, including but not limited to: data from all tests, system logs, execution logs, test director notes, certifications, and user/operator assessments and surveys. This applies to all government accessible data including classified, unclassified, and competition sensitive or proprietary data. Data may be preliminary and will be identified as such.

(2) The Program Manager and test agencies for all programs will provide the Defense Technical Information Center (DTIC) with all reports and the supporting data for the test events

in those reports. Paragraphs 11c(5) through 11c(7) in Enclosure 5 of this instruction include a more detailed discussion.

(3) The DoD Components will collect and retain data from developmental test and evaluation, integrated testing, and operational test and evaluation on the reliability and maintainability of Acquisition Category I and II programs.

(4) Reference (dc) identifies statutory and regulatory reporting and notification requirements associated with the conduct of DT&E.

ENCLOSURE 5

OPERATIONAL AND LIVE FIRE TEST AND EVALUATION (OT&E AND LFT&E)

1. OVERVIEW

a. The fundamental purpose of test and evaluation (T&E) is to enable the DoD to acquire systems that work. To that end, T&E provides engineers and decision-makers with knowledge to assist in managing risks, to measure technical progress, and to characterize operational effectiveness, suitability, and survivability. This is done by planning and executing a robust and rigorous T&E program.

b. The Program Manager is responsible for resourcing and executing the system's approved T&E program. The Program Manager assembles a test team of empowered representatives of the various test data consumers. The team starts early (i.e., pre-Milestone A) to develop a robust, rigorous, and efficient test program that will be conducted in support of systems engineering, evaluations, and certifications throughout the program life cycle. The Program Manager documents the test program planning in the Test and Evaluation Master Plan (TEMP). All TEMPs will require DoD Component approval; TEMPs for programs under DOT&E oversight will also require DOT&E approval. The operational and select live fire test events in the TEMP must have approved test plans. Test plans are written and approved by the test organization responsible for the test. Operational test plans (OTPs) for programs under DOT&E OT&E oversight and live fire test plans (LFTPs) for programs under DOT&E LFT&E oversight will require DOT&E approval.

c. For programs under DOT&E OT&E or LFT&E oversight, the DOT&E will provide the MDA with milestone assessments. DOT&E will submit a report to the Secretary of Defense and the congressional defense committees before programs under DOT&E OT&E or LFT&E oversight may proceed beyond Low-Rate Initial Production (LRIP), in accordance with 10 U.S.C. 2366 and 2399 (Reference (h)).

2. APPLICABILITY. This enclosure applies to all defense acquisition programs under OSD OT&E or LFT&E oversight. This enclosure is written to the Hardware Intensive Program model described in Reference (dc), with tailoring instructions for the software within those programs and the software-specific acquisition models. When there is no distinction between Defense Unique Software Intensive Programs (see Reference (dc)) and Incrementally Deployed Software Intensive Programs (see Reference (dc)), they are referenced herein as "Software Acquisitions." Tailoring for any software, irrespective of acquisition model, is identified as being "for software in any system." Tailoring for Accelerated Acquisition models will be considered on a case-by-case basis.

3. DOT&E OVERSIGHT LIST

a. DOT&E may place any program or system on the DOT&E Oversight List for OT&E or LFT&E oversight at any time.

b. DOT&E maintains the DOT&E Oversight List continuously online at https://extranet.dote.osd.mil/oversight/ (requires login with a Common Access Card).

c. The DOT&E Oversight List is unclassified. Classified and sensitive programs that are placed on DOT&E oversight will be identified directly to their MDAs.

d. The DOT&E Oversight List is the list of Major Defense Acquisition Programs (MDAPs) under DOT&E oversight. MDAPs on DOT&E oversight include those programs that meet the statutory definition of 10 U.S.C. 2430 (Reference (h)), and those that are designated by the DOT&E as MDAPs for the purposes of OT&E under the authority of paragraph (a)(2)(B) of 10 U.S.C. 139 (Reference (h)). The latter programs are not MDAPs for any other purpose.

e. Unless specifically waived, the test-related documentation that is required for MDAP programs will be required for all programs on the DOT&E Oversight List, including submission of Defense Intelligence Agency or DoD Component Validated On-line Life-cycle Threat Reports, TEMPs, OTPs, Live Fire Test Plans (LFTPs), and reporting of test results.

f. Force protection equipment (including non-lethal weapons) will be subject to DOT&E oversight, as determined by DOT&E. The DOT&E will approve required LFTPs and/or live fire strategies for such systems.

g. Capability upgrades, other alterations that materially change system performance, and alterations that pose substantial risk of degrading fielded military capabilities (if they fail) will be tested operationally. Product improvements or upgrades to system survivability will also be tested and evaluated.

h. The DOT&E Oversight List will identify programs grouped for coordinated or synchronized testing.

4. T&E PROGRAM MANAGEMENT

a. Early Engagement. Program managers for programs under DOT&E oversight will designate a T&E WIPT (also known as an Integrated Test Team), as soon as practicable after the Materiel Development Decision. The T&E WIPT develops and tracks the T&E program in all phases. The T&E WIPT will include empowered representatives of test data stakeholders such as Systems Engineering, Developmental Test and Evaluation (DT&E), OT&E, LFT&E, the user, Product Support, the intelligence community, and applicable certification authorities.

b. Lead Operational Test Agency (OTA). The lead OTA is the responsible OTA for a program. When more than one OTA is responsible for a program, the responsible OTAs will jointly identify the lead OTA.

c. Required Documentation. T&E program documentation that already exists in other acquisition documents may be provided by working links. Documentation that directly impacts the OT&E or LFT&E program will be included or linked in the applicable T&E documentation or else the documentation in question will be approved by DOT&E in addition to any other applicable approvals. DOT&E approval or disapproval of a document incorporating links constitutes approval or disapproval of the content applicable to operational testing in all of the links. Specifically, although DOT&E does not approve all the content of linked documents, DOT&E may require changes to linked content dealing specifically with operational or live-fire testing.

5. T&E PROGRAM PLANNING

a. The TEMP is a signed contract among DOT&E, senior DoD Component leadership, the lead OTA, the MDA, and the Program Manager.

b. The Program Manager and T&E WIPT will prepare and then update the TEMP to support the acquisition milestones. For the Full-Rate Production Decision Review or the Full Deployment Decision and thereafter (for DOT&E OT&E or LFT&E Oversight programs), DOT&E, the MDA, or the senior DoD Component leadership may require TEMP updates or addendums to address additional testing.

c. Working through the T&E WIPT, program managers for DOT&E oversight programs will make draft TEMPs available to program stakeholders as early and as frequently as possible. DoD Component-approved TEMPs will be submitted to OSD for approval not later than 45 calendar days prior to the milestone decision.

(1) A TEMP may be waived for select Accelerated or Urgent Acquisitions. In cases when DOT&E decides a TEMP is not needed, early briefings to DOT&E (in lieu of the TEMP) are recommended to facilitate subsequent DOT&E approval of the OTPs and LFTPs. DOT&E will approve the OTPs and LFTPs for accelerated acquisition (including capabilities acquired in response to an urgent need and acquisitions granted Rapid Acquisition Authority) if those acquisitions are under DOT&E OT&E or LFT&E oversight. If DOT&E has placed an Accelerated Acquisition on oversight, it is because DOT&E has determined that OT&E or LFT&E is required before fielding. Testing to verify safety, survivability, and operational performance will be conducted consistent with the urgency of deploying the capability. The Secretary of Defense may authorize the Rapid Acquisition Official to defer some testing until after fielding if he or she determines that the testing would unnecessarily impede the deployment of the needed capability. Testing should normally include user feedback to support design and operational use improvements.

(2) Initial Operational Test and Evaluation (IOT&E) is required for all programs under DOT&E oversight in accordance with 10 U.S.C. 2399 (Reference (h)). The lead OTA will conduct an independent, dedicated phase of IOT&E before full-rate production or full deployment that provides objective test results free from potential conflicts of interest or bias. The primary purpose of IOT&E is to determine a system's operational effectiveness and operational suitability. IOT&E can also be used to support system certification requirements and training requirements as long as the primary purpose is accomplished.

d. The lead OTA for the program and the Program Manager will initiate coordinated planning for IOT&E as early as possible so that developing activities will be aware of expectations at IOT&E:

(1) The lead OTA for the program will provide an assessment of the T&E implications of the initial concept of operations (CONOPS) provided by the user in the Milestone A TEMP.

(2) Beginning at Milestone A, the lead OTA will provide a working link in the TEMP to a living document in which the DoD Component's operational rationale for the requirements in the draft Capability Development Document (CDD) or equivalent requirements document will be tracked.

(3) For software acquisitions, the lead OTA will conduct an analysis of operational risk to mission accomplishment covering all planned capabilities or features in the system (see paragraph 7d in this enclosure for additional details). The analysis will include commercial and non-developmental items. The initial analysis will be documented in the Milestone A TEMP and updated thereafter.

(4) The TEMP will include evaluation of mission-level interoperability across key interfaces. Systems that provide capabilities for joint missions will be tested in the expected joint mission environment.

e. Scientific test and analysis techniques (also referred to as Design of Experiments methodologies) should be employed to design an effective and efficient T&E program. The TEMP should document the test program that will produce the required data to characterize combat mission capability across an appropriately selected set of factors and conditions.

(1) Starting at Milestone A, the TEMP should document T&E for phase completion (major test events required for milestone exit and entrance criteria). In addition, each major test phase or event should have test entrance and test completion criteria.

(2) Each major test phase or event should have a synopsis of the intended analysis. A synopsis should indicate how the required data for test completion will contribute to one or more standard measures of program progress. These include the following terms:

(a) Critical operational issues (also known as critical operational issues and criteria).

(b) KPPs.

(c) Critical technical parameters.

(d) Key system attributes.

(3) Every TEMP will include a table of independent variables (or "conditions," "parameters," "factors," etc.) that may have a significant effect on operational performance. Starting at Milestone B, the updated table of variables will include the anticipated effects on operational performance, the range of applicable values (or "levels," "settings," etc.), the overall priority of understanding the effects of the variable, and the intended method of controlling the variable during test (uncontrolled variation, hold constant, or controlled systematic test design).

(4) Starting at Milestone B, every TEMP will include an evaluation overview. The overview will show how the major test events and test phases link together to form a systematic, rigorous, and structured approach to evaluating mission capability across the applicable values of the independent variables. Test resources will be derived from the evaluation overview (see section 10 in this enclosure).

6. OT&E ACTIVITIES

a. Operational Assessments (OAs)

(1) The lead OTA will prepare and report results of one or more early OAs (EOAs) as appropriate in support of one or more of the design phase life-cycle events (namely, the CDD Validation, the Development RFP Release Decision Point, or Milestone B). An EOA is typically an analysis, conducted in accordance with an approved test plan, of the program's progress in identifying operational design constraints, developing system capabilities, and mitigating program risks. For programs that enter development at Milestone B, the lead OTA will (as appropriate) prepare and report EOA results after program initiation and prior to the Critical Design Review.

(2) An OA is a test event that is conducted before initial production units are available and which incorporates substantial operational realism. An OA is conducted by the lead OTA in accordance with a test plan approved by DOT&E for programs that are under OSD OT&E oversight. As a general criterion for proceeding through Milestone C, the lead OTA will conduct and report results of at least one OA. For an acquisition program employing the Incrementally Deployed Software Intensive Program model, a risk-appropriate OA is usually required in support of every limited deployment (see Reference (dc)). An operational test, usually an OA, is required prior to deployment of accelerated or urgent acquisition programs that are under OSD OT&E or LFT&E oversight. An OA may be combined with training events (see paragraph 11a(9) in this enclosure). An OA is not required for programs that enter the acquisition system at Milestone C.

b. RFPs. An up-to-date TEMP will be provided prior to release of RFPs for Milestone B and Milestone C. To the maximum extent feasible, RFPs should be consistent with the operational test program documented in the TEMP.

c. OT&E for Reliability and Maintainability

(1) The TEMP will include a plan (typically via working link to the Systems Engineering Plan) to allocate top-level reliability requirements down to the components and sub-components. Reliability allocations will include hardware and software, and will include commercial and non-development items.

(2) Reliability Growth

(a) Beginning at Milestone B, the TEMP will include T&E for reliability growth and reliability growth curves (RGCs) for the whole system and the reliability of critical systems, sub-systems, components, and sub-components. Reliability-critical items require test to mitigate risk resulting from the use of new technologies or from challenging operating environments. T&E for reliability growth will provide data on initial reliability (namely: identify the contractor and government reliability testing needed to achieve initial reliability) and reliability test events. RGCs will display planned initial reliability, the allocated reliability requirement, a curve showing reliability that is expected during each reliability test event, and points marking reliability test results to date.

(b) For software (in any system) reliability growth will be measured by software maturity metrics (e.g., counts of high priority defects) at regular intervals.

(c) Beginning at Milestone B, the TEMP will include a working link to the Failure Modes, Effects and Criticality Analysis (FMECA) of identified or anticipated system failure modes, the impacted components and sub-components, and the method of failure mode discovery. A software defect or failure tracking database(s) may replace the FMECA in software acquisitions.

(3) Updated TEMPs at Milestone C will include updated RGCs that reflect test results to date, any updates to the planned T&E for reliability growth, and a working link to the updated FMECA.

d. Use of Modeling and Simulation. Models or simulations that utilize or portray threat characteristics or parameters must have that portrayal accredited by the Defense Intelligence Agency. Every distinct use of a model or simulation in support of an operational evaluation will be accredited by an OTA, and, for programs under DOT&E Oversight, its use for the operational evaluation will be approved by DOT&E.

7. OT&E FOR SOFTWARE

a. Acquisition of software for any system will normally be supported by specialized models and early user involvement:

(1) As feasible, testing of software for any system should be supported by a model (or emulated hardware or virtual machine) of the digital device(s) on which the software runs.

(2) To the extent feasible, program managers should test prototype human interfaces with operational users.

(3) Program managers for software acquisitions should develop process models of the time and effort needed to perform critical tasks and functions. Such models support operational test design and analysis of results as well as managerial needs such as sustainment cost projections and analysis of impacts of process changes.

(4) Program managers must sustain an operationally realistic maintenance test environment in which software patches can be developed and upgrades of all kinds (developed or commercial) can be tested. The maintenance test environment is a model of the operational environment in that it should be able to replicate software defects found in the operational environment.

b. Program managers for software acquisitions will provide plans at Milestone B indicating how system logs and system status records will interface with operational command and control. At IOT&E or a prior test event, program managers for software acquisitions will demonstrate performance monitoring of operational metrics to manage and operate each system capability (or the whole system, as appropriate).

c. For software in any system, the evaluation of operational suitability will include a demonstrated capability to maintain the software. IOT&E or a prior test event will include an end-to-end demonstration of regression test, preferably automated, in the maintenance test environment. The demonstration will show how changes in requirements or discovered defects are mapped to lines of software that must be modified, and how modifications in software are mapped to the regression test scripts that will verify correct functioning of the modified software.

d. Risk-Assessed Level of Operational Test for Software Acquisitions (Models 3, 4, and Hybrids)

(1) OT&E for software acquisitions will be guided by the assessment of operational risks of mission failure. A significant operational risk of mission failure is a risk that is at least moderately likely to occur, and if the risk does occur then the impact will cause a degradation or elimination of one or more operational capabilities.

(2) At any level of risk, the lead OTA will coordinate with DOT&E on the required level of test and then observe the agreed-upon testing. At the lowest risk level, the lead OTA will review plans and observe developmental testing or developmental testing and integrated testing. At the highest risk level, the lead OTA will execute a full OT&E in accordance with the DOT&E-approved OTP. For intermediate risks, the lead OTA will coordinate with the responsible developmental testing organization to observe and execute some integrated developmental testing/operational testing in accordance with a DOT&E-approved OTP.

(3) DOT&E will require an operational test or OA for every Limited Deployment in any acquisition model. The scope of the OT&E or OA will be guided by the risk of capability being fielded or deployed.

(4) IOT&E is required for every increment, in any acquisition model (except as noted for urgent operational needs). IOT&E will normally occur prior to the Full Deployment Decision. IOT&E will be guided by an updated assessment of the operational risks in the capabilities and system interactions that have not been successfully evaluated in previous operational testing.

8. CYBERSECURITY.

a. Beginning at Milestone A, the TEMP will document a strategy and resources for cybersecurity T&E. At a minimum, software in all systems will be assessed for vulnerabilities. Mission critical systems or mission critical functions and components will also require penetration testing from an emulated threat in an operationally realistic environment during OT&E.

b. Beginning at Milestone B, appropriate measures will be included in the TEMP and used to evaluate operational capability to protect, detect, react, and restore to sustain continuity of operation. The TEMP will document the threats to be used, which should be selected based on the best current information available from the intelligence community.

c. The Program Manager, T&E subject matter experts, and applicable certification stakeholders will assist the user in writing testable measures for cybersecurity and interoperability.

d. The Program Manager and OTA will conduct periodic cybersecurity risk assessments to determine the appropriate Blue/Green/Red Team, and operational impact test events in alignment with the overall test strategy for evaluating the program for real world effects. Defense business systems will undergo Theft/Fraud operational impact testing.

9. LFT&E. 10 U.S.C. 2366 (Reference (h)) mandates the LFT&E and formal LFT&E reporting for all covered systems, as determined by DOT&E, including Accelerated Acquisitions, survivability improvement, and kit programs to address urgent needs. DOT&E will require approval of LFT&E strategies and LFT&E test plans (including survivability test plans) for covered systems as defined in section 2366. The DOT&E will determine the quantity of test articles procured for all LFT&E test events for any system under DOT&E LFT&E oversight.

10. RESOURCES AND SCHEDULE. All TEMPs will identify the resources needed to execute the planned T&E activities. Resource estimates will be matched against the schedule and justified by analysis in the TEMP. All TEMPs will contain an updated integrated test program summary and master schedule of all major test events or test phases, to include LFT&E events.

a. Resource estimates (including but not limited to quantities of test articles, targets, expendables, threat simulations, operational forces, etc.) will be derived from defensible statistical measures of merit (power and confidence) associated with quantification of the differences among the factors affecting operational performance as well as the risk to the government of accepting a poorly performing system or incorrectly rejecting a system with acceptable performance. Specifically, the TEMP must discuss and display, or provide a reference to, the calculations done to derive the content of testing and to develop the associated resource estimates.

b. The Program Manager and the Services or Defense Agencies will allocate the resources identified in the TEMP. Each TEMP update will include an updated and complete T&E resource estimate.

c. Test infrastructure, resources (including threat representations), and tools to be used in operational tests must undergo verification by the developer, validation by the DoD Component, and accreditation by the OTA. Test infrastructure, resources, and tools, and their associated verification, validation, and accreditation strategies will be documented in the TEMP.

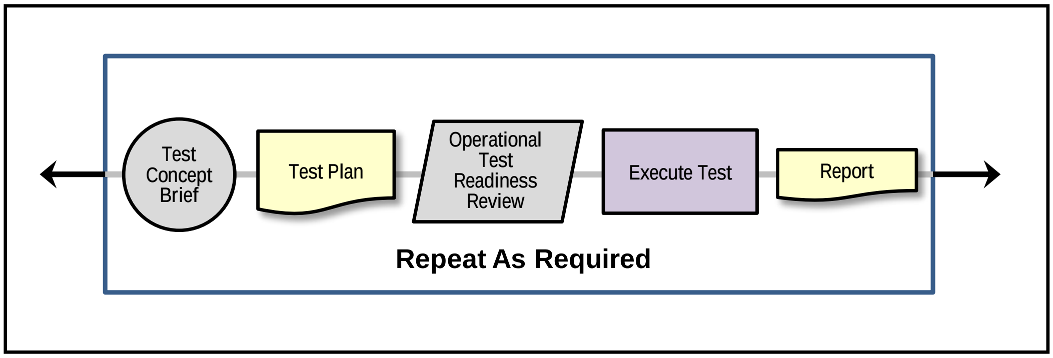
d. In accordance with 10 U.S.C. 2399 (Reference (h)), DOT&E will approve the quantity of test articles required for all operational test events for any system under DOT&E oversight. The DoD Component OTA will determine the quantity for programs that are not under DOT&E oversight.

e. The T&E schedule will be event-driven and allow adequate time to support pre-test predictions; testing; post-test analysis, evaluation, and reporting; reconciliation of predictive models; and adequate time to support execution of corrective actions in response to discovered deficiencies.

f. For incremental software acquisitions employing limited deployments (see Reference (dc)), the Milestone B TEMP will show a general schedule for the routine test sequence (developmental tests, certifications, integrated and operational tests) that will occur with every limited deployment within the allotted time for each limited deployment.

11. OPERATIONAL AND LIVE FIRE T&E EXECUTION. The general process for planning, executing, and reporting on operational and major live fire test events is shown in Figure 1.

Figure 1. Operational or Major Live Fire Test Event: Planning, Approval, Execution, and Reporting



a. Planning Test Events

(1) For all programs under DOT&E oversight, including Accelerated Acquisitions, DOT&E will approve OTPs and LFTPs prior to the corresponding operational or major live fire test events in accordance with 10 U.S.C. 2399. DOT&E will approve any LFTP for a major test event such as Full-up System Level test, Total Ship Survivability Trial, or Full Ship Shock Trials. The major live fire test events will be identified in the TEMP (or LFT&E strategy or equivalent document). Test plans are developed by a lead test organization (LTO). The LTO is the lead OTA for OT&E. The LTO varies for LFT&E.

(2) For programs under DOT&E oversight, the appropriate LTO will brief the DOT&E on T&E concepts for the OTP or the major LFT&E as early as possible and not less than 180 calendar days prior to start of any such testing. DOT&E and DoD Component leads will be kept apprised of changes in test concept and progress on the OTP. The lead OTA will deliver the DoD Component-approved OTP for DOT&E review not later than 60 calendar days before test start. The LTO for major live fire events will deliver the DoD Component-approved LFTP for DOT&E review not later than 90 days before test start.

(3) OTPs and major LFTPs will include the plans for data collection and management.

(4) Integrated Testing

(a) Integrated testing is the collaborative planning and collaborative execution of test phases and events to provide shared data in support of independent analysis, evaluation and reporting by all stakeholders particularly the developmental (both contractor and government) and operational test and evaluation communities. It requires the active participation of the lead OTA in planning the integrated tests with the program office so that the operational objectives are understood, the testing is conducted in an operationally realistic manner, and the resultant data is relevant for use in operational evaluations.

(b) For integrated test results to count for operational testing, the lead OTA must develop a plan for the integrated test to be approved by DOT&E before the start of testing that, at a minimum, details the required test realism and conditions, operational test objectives, operational test metrics and data collection requirements. Data collected outside an approved OTP or major LFTP can be used for a DOT&E operational or live fire evaluation if the data is approved by DOT&E. Depending on circumstances, DOT&E approval will not necessarily be possible in the TEMP and may require some other documentation. Data approval will be based on understanding of the realism of the test scenario(s) used and the pedigree (test conditions and methodologies) of the data. The data in question will typically come from operational exercises, certification events, and developmental test events conducted in operationally relevant environments. Data approval should be coordinated with the LTO and DOT&E prior to the start of testing. When advance coordination is not possible, the LTO will facilitate data re-use (in a DOT&E assessment or evaluation) through independent documentation of the test data pedigree (test conditions and methodologies).

(5) In OT&E, typical users or units will operate and maintain the system or item under conditions simulating combat stress in accordance with 10 U.S.C. 139 (Reference (h)) and peacetime conditions, when applicable. The lead OTA, in consultation with the user and the Program Manager, will identify realistic operational scenarios based on the CONOPS (per paragraph 5d(1) in this enclosure) and mission threads derived from the Joint Mission Essential Task List or DoD Component-specific Mission Essential Task List. See paragraph 7d of this enclosure for risk-assessed OT&E of software acquisitions.

(6) In accordance with 10 U.S.C. 2399 (Reference (h)), persons employed by the contractor for the system being developed may only participate in OT&E of systems under OSD OT&E oversight to the extent they are planned to be involved in the operation, maintenance, and other support of the system when deployed in combat.

(a) A contractor that has participated (or is participating) in the development, production, or testing of a system for a DoD Component (or for another contractor of the DoD) may not be involved in any way in establishing criteria for data collection, performance assessment, or evaluation activities for OT&E.

(b) These limitations do not apply to a contractor that has participated in such development, production, or testing, solely in test or test support on behalf of the DoD.

(7) IOT&E for all programs will use production or production-representative test articles that, at a minimum, will incorporate the same parts and software items to be used in LRIP articles. Production-representative systems meet the following criteria:

(a) The hardware and software must be as defined by the system-level critical design review, functional configuration audit, and system verification review, including correction of appropriate major deficiencies identified during prior testing.

(b) For hardware acquisitions, production-representative articles should be assembled using the parts, tools, and manufacturing processes intended for use in full-rate production; utilize the intended production versions of software; and the operational logistics systems including mature drafts of maintenance manuals intended for use on the fielded system should be in place. The manufacturing processes to be used in full-rate production should be adhered to as closely as possible, and program managers for programs under DOT&E OT&E oversight will provide DOT&E a detailed description of any major manufacturing process changes.

(c) For software acquisitions, a production-representative system consists of typical users performing operational tasks with the hardware and software intended for deployment, in an operationally realistic computing environment, with representative DoD information network operations and supporting cybersecurity capabilities. All manuals, training, helpdesk, continuity of operations, system upgrade and other life-cycle system support should be in place.

(8) IOT&E will require more than an evaluation that is based exclusively on computer modeling, simulation, or an analysis of system requirements, engineering proposals, design specifications, or any other information contained in program documents in accordance with 10

U.S.C. sections 2399 and 2366 (Reference (h)). IOT&E will feature end-to-end testing of system capabilities including all interrelated systems needed to employ and support those capabilities.

(9) Program managers for all programs (and particularly Accelerated Acquisitions) may, in coordination with the lead OTA, elect to perform integrated testing in conjunction with training, joint and operational exercises, or synchronized test events. Such testing is efficient, but inherently increases the risk that a significant problem will not be discovered. If no subsequent operational testing is conducted prior to fielding, then additional testing will typically be required subsequent to initial fielding. When subsequent testing is required, the plan for the T&E and reporting of results will be included in the applicable TEMP or other planning documentation.

b. Conducting Test Events

(1) Test plans must consider the potential impacts on personnel and the environment, in accordance with 42 U.S.C. 4321-4347 (Reference (ag)) and Executive Order 12114 (Reference (ah)). The Program Manager, working with the user and the T&E community, will provide safety releases (to include formal environment, safety, and occupational health risk acceptance in accordance with section 16 of Enclosure 3 of this instruction) to the developmental and operational testers prior to any test that may impact safety of personnel.

(2) Barring significant unforeseen circumstances, all elements of an approved OTP or LFTP must be fully satisfied by the end of an operational or live fire test. If an approved plan cannot be fully executed, DOT&E concurrence with any changes must be obtained before revised test events are executed. Once testing has begun, deviations from approved elements of the test plan cannot be made prior to the beginning of their execution without consultation with the OTA commander (for OTP) or appropriate LTO (for LFTP) and the concurrence of DOT&E. DOT&E concurrence is not required when a need to change the execution of an element of the test plan arises in real time as its execution is underway. If DOT&E on-site representatives are not present and the test director concludes changes to the plan are warranted that would revise events yet to be conducted, the test director must contact the relevant DOT&E personnel to obtain concurrence with the proposed changes. If it is not possible to contact DOT&E personnel in a timely manner, the test director can proceed with execution of the revised test event but must inform DOT&E of the deviations from the test plan as soon as possible.

(3) When the order of execution is identified in the TEMP as affecting the analysis of the data, test plans should include details on the order of test event execution and/or test point data collection.

(4) Operating instructions (i.e., tactics, techniques and procedures, standard operating procedures, technical manuals, technical orders) should be considered for their impact on the test outcomes and included in OTPs when relevant.

(5) Test plans must include the criteria to be used to make routine changes (delays for weather, test halts, etc.).

(6) If required data for the test completion criteria are lost, corrupted, or not gathered, then the test is not complete unless the requirement is waived by DOT&E.

c. Data Management, Evaluation, and Reporting

(1) DOT&E, the Program Manager and their designated representatives who have been properly authorized access, will all have full and prompt access to all records, reports, and data, including but not limited to data from tests, system logs, execution logs, test director notes, and user and operator assessments and surveys. Data include but are not limited to classified, unclassified, and (when available) competition sensitive or proprietary data. Data may be preliminary and will be identified as such.

(2) OTAs and other T&E agencies will record every OT&E and LFT&E event in some written form. Full reports will often contain multiple test events and will be accomplished in the most timely manner practicable. Interim summaries or catalogues of individual events will be prepared as results become available.

(3) Significant problems will be reported promptly to senior DoD leadership when those problems are identified. OTAs will publish interim test event summaries as interim reports when the test events provide information of immediate importance to the program decision makers. This will occur particularly in support of accelerated acquisitions and time critical operational needs. Such reports should provide the most complete assessment possible based on the available data and should not be delayed. Such reports will be followed by the planned comprehensive reporting.

(4) For DOT&E OT&E and LFT&E oversight programs, DOT&E will be kept informed of available program assets, assessments, test results and anticipated timelines for reporting throughout report preparation.

(5) The Program Manager and test agencies for all programs will provide the Defense Technical Information Center (DTIC) with all reports, and the supporting data and metadata for the test events in those reports. If there are limitations in the data or metadata that can be provided to DTIC, those limitations will be documented in the TEMP starting at Milestone B.

(6) Test agencies will provide the DoD Modeling and Simulation Coordination Office with a descriptive summary and metadata for all accredited models or simulations that can potentially be reused by other programs.

(7) The Secretaries of the Military Departments, in coordination with the Defense Acquisition Executive, DOT&E, and the Under Secretary of Defense for Personnel and Readiness, will establish a common set of data for each major weapon system type to be collected on damage incurred during combat operations. This data will be stored in a single dedicated and accessible repository at DTIC. The lessons learned from analyzing this data will be included, as appropriate, in both the capability requirements process and the acquisition process for new acquisitions, modifications, and/or upgrades.

12. OPERATIONAL TEST READINESS. The DoD Components will each establish an Operational Test Readiness Review process to be executed for programs under DOT&E oversight prior to any Operational Test. Prior to IOT&E, the process will include a review of DT&E results, an assessment of the system's progress against the KPPs, key system attributes, and critical technical parameters in the TEMP, an analysis of identified technical risks to verify that those risks have been retired or mitigated to the extent possible during DT&E and/or OT&E, a review of system certifications, and a review of the IOT&E entrance criteria specified in the TEMP.

13. CERTIFICATIONS. Testing in support of certifications should be planned in conjunction with all other testing.

a. The Program Manager is responsible for determining what certifications are required; ensuring involvement of the representatives of applicable certifying authorities in the T&E WIPT; and satisfying the certification requirements.

b. The Program Manager will provide the MDA, DOT&E, and the lead OTA with all data on certifications as requested.

c. In accordance with DoD Instruction 8330.01 (Reference (ab)), the TEMP for all programs must reflect interoperability and supportability requirements, and serve as the basis for interoperability assessments and certifications.

14. TEMP EVOLUTION THROUGH THE ACQUISITION MILESTONES. The preceding policies are summarized together with associated DOT&E guidance and TEMP outlines at http://www.dote.osd.mil/temp-guidebook/index.html.

ENCLOSURE 6

LIFE-CYCLE SUSTAINMENT

Enclosure 6 was removed through formal coordination and approval of Reference (dc); necessary information can be found in that issuance.

ENCLOSURE 7

HUMAN SYSTEMS INTEGRATION (HSI)

1. PURPOSE. This enclosure describes the HSI policy and procedure applicable to defense acquisition programs.

2. GENERAL. The Program Manager will plan for and implement HSI beginning early in the acquisition process and throughout the product life cycle. The goal will be to optimize total system performance and total ownership costs, while ensuring that the system is designed, operated, and maintained to effectively provide the user with the ability to complete their mission. Program Managers will ensure that the DoD Component HSI staff is aware of and engaged with WIPTs tasked with the development and review of program planning documents that reflect HSI planning and inform program decisions.

3. HSI PLANNING. HSI planning and implementation will address the following seven HSI domains recognized by the DoD:

a. Human Factors Engineering. The Program Manager will take steps (e.g., contract deliverables and government/contractor integrated product teams) to ensure ergonomics, human factors engineering, and cognitive engineering is employed during systems engineering over the life of the program to provide for effective human-machine interfaces and to meet HSI requirements. System designs will minimize or eliminate system characteristics that require excessive cognitive, physical, or sensory skills; entail extensive training or workload-intensive tasks; result in mission-critical errors; or produce safety or health hazards.

b. Personnel. The Program Manager will, in conjunction with designated DoD Component HSI staff, define the human performance characteristics of the user population based on the system description, projected characteristics of target occupational specialties, and recruitment and retention trends. To the extent possible, systems will not require special cognitive, physical, or sensory skills beyond that found in the specified user population. For those programs that have skill requirements that exceed the knowledge, skills, and abilities of current military occupational specialties, or that require additional skill indicators or hard-to-fill military occupational specialties, the Program Manager will consult with personnel communities to mitigate readiness, personnel tempo, and funding issues.

c. Habitability. The Program Manager will, in conjunction with designated DoD Component staff, establish requirements for the physical environment (e.g., adequate space and temperature control) and, if appropriate, requirements for personnel services (e.g., medical and mess) and living conditions (e.g., berthing and personal hygiene) for conditions that have a direct impact on meeting or sustaining system performance or that have such an adverse impact on quality of life and morale that recruitment or retention is degraded.

d. Manpower. In advance of contracting for operational support services, the Program Manager will, in conjunction with the designated DoD Component manpower authority, determine the most efficient and cost-effective mix of DoD manpower and contract support. The mix of military, DoD civilian, and contract support necessary to operate, maintain, and support (to include providing training) the system will be determined based on the manpower mix criteria (see DoD Instruction 1100.22 (Reference (bm))). Manpower mix data will be reported to cost analysts and factored into the preparation of independent cost estimates and DoD Component cost estimates. Economic analyses used to support workforce mix decisions will use costing tools, to include DoD Instruction 7041.04 (Reference (bn)), that account for fully loaded costs (i.e., all variable and fixed costs, compensation and non-compensation costs, current and deferred benefits, and cash and in-kind benefits) approved by the DoD Component manpower authority.

e. Training. The Program Manager will, in conjunction with designated DoD Component staff, develop options for individual, collective, and joint training for operators, maintenance and support personnel, and, where appropriate, base training decisions on training effectiveness evaluations (which can be integrated with other test and evaluation). The major tasks identified in the job task analysis, training device document coordinating paper and training plans will support a comprehensive analysis with special emphasis on options that enhance user capabilities, maintain skill proficiencies, and reduce individual and collective training costs. The Program Manager will develop training system plans that consider the use of new learning techniques, simulation technology, embedded training and distributed learning, and instrumentation systems that provide “anytime, anyplace” training and reduce the demand on the training establishment. Where cost effective and practical, the Program Manager will use simulation-supported embedded training, and the training systems will fully support and mirror the interoperability of the operational system in accordance with DoD Directive 1322.18 (Reference (bo)).

f. Safety and Occupational Health. The Program Manager will ensure that appropriate HSI and environmental, safety, and occupational health efforts are integrated across disciplines and into systems engineering to determine system design characteristics that can minimize the risks of acute or chronic illness, disability, or death or injury to operators and maintainers; and enhance job performance and productivity of the personnel who operate, maintain, or support the system.

g. Force Protection and Survivability. The Program Manager will assess risks to personnel and address, in terms of system design, protection from direct threat events and accidents (such as chemical, biological, and nuclear threats). Design consideration will include primary and secondary effects from these events and consider any special equipment necessary for egress and survivability.

ENCLOSURE 8

AFFORDABILITY ANALYSIS AND INVESTMENT CONSTRAINTS

Enclosure 8 was removed through formal coordination and approval of Reference (dc); necessary information can be found in that issuance.

ENCLOSURE 9

ANALYSIS OF ALTERNATIVES (AOA)

Enclosure 9 was removed through formal coordination. Necessary information can be found in Reference (bp) or in the Defense Acquisition Guidance.

ENCLOSURE 10

COST ESTIMATING AND REPORTING

Enclosure 10 was removed through formal coordination. Necessary information is available in Reference (w).

ENCLOSURE 11

REQUIREMENTS APPLICABLE TO ALL PROGRAMS CONTAINING INFORMATION TECHNOLOGY (IT)

Enclosure 11 was removed through formal coordination and approval of Reference (da); necessary information can be found in that issuance.

ENCLOSURE 12

URGENT CAPABILITY ACQUISITION

Enclosure 12 was removed through formal coordination and approval of Reference (de); necessary information can be found in that issuance.

ENCLOSURE 13

CYBERSECURITY IN THE DEFENSE ACQUISITION SYSTEM

1. PROGRAM MANAGER RESPONSIBILITIES. Program managers, assisted by supporting organizations to the acquisition community, are responsible for the cybersecurity of their programs, systems, and information. This responsibility starts from the earliest exploratory phases of a program, with supporting technology maturation, through all phases of the acquisition. Acquisition activities include system concept trades, design, development, test and evaluation (T&E), production, fielding, sustainment, and disposal. Program managers will pay particular attention to the following areas where a cybersecurity breach or failure would jeopardize military technological advantage or functionality:

a. Program Information. This includes, but is not limited to:

(1) Information about the acquisition program, personnel, and the system being acquired, such as planning data, requirements data, design data, test data, operational software data, and support data (e.g., training, maintenance data) for the system.

(2) Information that alone might not be damaging and might be unclassified, but that in combination with other information could allow an adversary to compromise, counter, clone, or defeat warfighting capability or to simply gain a cost and schedule advantage.

b. Organizations and Personnel. This includes government program offices, manufacturing, testing, depot, and training organizations, as well as the prime contractors and subcontractors supporting those organizations.

c. Enabling Networks. This includes government and government support activity unclassified and classified networks, contractor unclassified and classified networks, and interfaces among government and contractor networks.

d. Systems, Enabling Systems, and Supporting Systems. This includes systems in acquisition, enabling systems that facilitate life cycle activities (e.g., manufacturing, testing, training, logistics, maintenance), and supporting systems that contribute directly to operational functions (e.g., interconnecting operational systems).

2. ACTIVITIES TO MITIGATE CYBERSECURITY RISKS. Program Managers will rely on existing cybersecurity standards tailored to reflect analysis of specific program risks and opportunities to determine the level of cyber protections needed for their program information, the system, enabling and support systems, and information types that reside in or transit the fielded system. Appropriate cyber threat protection measures include information safeguarding, designed in system protections, supply chain risk management (SCRM), software assurance, hardware assurance, anti-counterfeit practices, anti-tamper (AT), and program security related

activities such as information security, operations security (OPSEC), personnel security, physical security, and industrial security.

a. Safeguard Program Information Against Cyber-Attack. Program Managers will:

(1) Ensure Federal Acquisition Regulation (FAR) Clause 52.204-2 (Reference (ak)) is included in solicitations and contracts that may require access to classified information; conduct assessments of compromised classified information, and mitigate impacts as a result of the loss of information.

(2) Ensure FAR Clause 52.204-21 is included in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.

(3) Ensure Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 (Reference (al)) is included in all solicitations and contracts, including solicitations and contracts using Part 12 of the FAR procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of commercially available off-the-shelf items. Use other appropriate DFARS and FAR requirements for solicitations and contracts that include the clause; and if a cyber incident is reported, assess what unclassified CDI was compromised, and mitigate impacts as a result of the loss of CDI.

(4) Assess unclassified controlled technical information losses associated with cyber incidents reported under contracts that contain DFARS Clause 252.204–7012. Refer to the Guidance to Stakeholders for Implementing DFARS Clause 252.204-7012 for detailed guidance on these assessments. Use the Joint Acquisition Protection and Exploitation Cell (JAPEC) to assist in tracking and correlating threat intelligence reports to further inform courses of action.

b. Design for Cyber Threat Environments. In order to design, develop, and acquire systems that can operate in applicable cyber threat environments, Program Managers will:

(1) Identify the digitized T&E data that will contribute to assessing progress toward achieving cybersecurity requirements. The T&E strategy should include not only the explicit cybersecurity requirements, but also all key interfaces. This is the key first step of the T&E planning process to support design and development. To support the architecture and design considerations in paragraph 3b(2)(a) of this enclosure, determine the avenues and means by which the system and supporting infrastructure may be exploited for cyber-attack and use this information to design T&E activities and scenarios.

(2) Apply DoDIs 8500.01 (Reference (x)) and 8510.01 (Reference (bg)) in accordance with DoD Component implementation and governance procedures. Program Managers will use program protection planning, system security engineering, developmental test and evaluation (DT&E), sustainment activities, and cybersecurity capabilities or services external to the system (e.g., common controls) to meet risk management framework for DoD IT objectives. Program Managers will collaborate with designated authorizing officials from program inception and

throughout the life cycle, to ensure system and organizational cybersecurity operations are in alignment, and to avoid costly changes late in a program's development.

(3) Establish, implement, and sustain security configuration parameters (e.g., Defense Security Technical Implementation Guides or Security Requirements Guides) for the system.

(4) Plan for and resource cybersecurity T&E in order to identify and eliminate as many cybersecurity shortfalls as early in the program as possible. Refer to the "Department of Defense Cybersecurity Test and Evaluation Guidebook" (Reference (cr)) and the Director of Operational Test and Evaluation (DOT&E) "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," (Reference (cs)) for detailed guidance on cybersecurity T&E planning. Beginning early, before Milestone A, work closely with the Chief Developmental Tester as well as the T&E WIPT to plan, as described in paragraph 3b(2), this enclosure, and conduct cybersecurity T&E, as described in paragraphs 3b(13)(a) and 3b(13)(b), this enclosure, to provide feedback to design and engineering teams. This will help avoid costly and difficult system modifications late in the acquisition life cycle. Cybersecurity T&E spans the entire material life cycle of the program, and each phase builds off the completion of the prior phase. T&E activities should be planned for and documented in the Test and Evaluation Master Plan (TEMP), including the T&E Strategy, evaluation frameworks (DT&E and operational T&E), and resource requirements. Cybersecurity T&E will include:

(a) <u>Developmental Testing</u>

<u>1</u>. <u>Cooperative Vulnerability Identification</u>. Conduct T&E activities to collect data needed to identify vulnerabilities and plan the means to mitigate or resolve them, including system scans, analysis, and architectural reviews.

<u>2</u>. <u>Adversarial Cybersecurity DT&E</u>. Conduct a cybersecurity DT&E event using realistic threat exploitation techniques in representative operating environments and scenarios to exercise critical missions within a cyber-contested environment to identify any vulnerabilities.

(b) <u>Operational Testing</u>. Two phases of cybersecurity testing are required as part of operational testing for all systems under the oversight of the Director of Operational Test and Evaluation. Program Managers should coordinate with the appropriate operational test agency to prepare their systems for these assessments by conducting comprehensive cybersecurity testing during system development.

<u>1</u>. <u>Cooperative Vulnerability and Penetration Assessment</u>. This phase consists of an overt examination of the system to identify all significant vulnerabilities and the risk of exploitation of those vulnerabilities. This assessment is conducted in cooperation with the system's Program Manager. It is a comprehensive characterization of the cybersecurity status of a system in a fully operational context, and may be used to substitute for reconnaissance activities in support of adversarial testing when necessary. The assessment should consider the operational implications of vulnerabilities as they affect the capability to protect system data, detect unauthorized activity, react to system compromise, and restore system capabilities. This

testing may be integrated with DT&E activities if conducted in a realistic operational environment, and if the DOT&E approves the testing in advance.

2. Adversarial Assessment. This phase assesses the ability of a unit equipped with a system to support its mission while withstanding cyber threat activity representative of an actual adversary. In addition to assessing the effect on mission execution, the test must evaluate the ability to protect the system and data, detect threat activity, react to threat activity, and restore mission capability degraded or lost due to threat activity. This test phase should be conducted by an operational test agency employing a National Security Agency-certified adversarial team to act as a cyber aggressor presenting multiple cyber intrusion vectors consistent with the expected threat. The assessment should characterize the system's vulnerability as a function of an adversary's cyber experience level, relevant threat vectors, and other pertinent factors.

c. Manage Cybersecurity Impacts to Information Types and System Interfaces to the DoDIN. Information types include specific categories of information resident in or transiting fielded systems (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management), defined by an organization or, in some instances, by a public law, E.O., directive, policy, or regulation. Program Managers will:

(1) Use applicable DoD and Component issuances, and specific program situations to tailor cybersecurity activities and guide collaboration throughout the system life cycle between the Program Manager team and the entities responsible for ensuring an acceptable cybersecurity posture during operations.

(2) Incorporate Federal Information Processing Standards, or National Security Agency/Central Security Service (NSA/CSS)-certified cryptographic products and technologies into systems in order to protect information types at rest and in transit. Programs with certain cryptographic requirements, as determined by the information type or other protection considerations, must coordinate development efforts with NSA/CSS Information Assurance Directorate.

3. PROTECTION PLANNING

a. Systems Engineering Plan (SEP). Program Managers will ensure the SEP, developed in accordance with Enclosure 3 of this instruction, describes the program’s overall technical approach to cybersecurity and related program security, including technical risk, processes, resources, organization, metrics, and design considerations.

b. PPP. In accordance with Enclosure 3 of this instruction, Program Managers will prepare a PPP as a management tool to guide the program and systems security engineering, to include cybersecurity, activities across the life cycle. The PPP will be submitted for MDA approval at each milestone review, beginning with Milestone A.

(1) Program Managers should ensure the PPP is included in requests for proposals (RFPs) and prepare updates to the PPP after any contract award to reflect the contractor's approved technical approach, and after identification of any significant threat activity or compromise.

(2) After the full rate production or full deployment decision, the PPP will transition to the Program Manager responsible for system sustainment and disposal.

c. TEMP. Ensure planned cybersecurity T&E as described in the TEMP, developed in accordance with Enclosures 4 and 5 of this instruction, includes activities that produce data to support engineering, risk management and acquisition decisions. Include within the T&E strategy those elements and interfaces of the system that, based on criticality and vulnerability analysis, need specific attention in T&E events. Vulnerability testing and evaluation must be planned for and described within the TEMP, and included as appropriate in RFPs and government DT&E.

d. Risk Management Framework for DoD IT Security Plan and Cybersecurity Strategy. As tailored to specific program situations, Program Managers will prepare plans and strategies in accordance with DoDI 8510.01 (Reference (bg)) and applicable DoD Component issuances.

4. RESOURCES FOR EXECUTING CYBERSECURITY AND RELATED PROGRAM SECURITY ACTIVITIES. Table 2 lists and describes various resources and publications available for the Program Manager to use in executing cybersecurity and related program security procedures detailed in this enclosure.

Table 2. Cybersecurity and Related Program Security Resources and Publications

Category	Title of Resource and Description
Information Protection	FAR Clause 52.204-2 (Reference (ak)) This clause applies to the extent that the contract involves access to information classified Confidential, Secret, or Top Secret. The clause is related to compliance with the National Industrial Security Operating Manual and any revisions to that manual for which notice has been furnished to a contractor.
Protection of Information on Networks	FAR Clause 52.204-21 (Reference (ak)) This clause applies to information not intended for public release that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Websites) or simple transactional information, such as necessary to process payments.
	DFARS Clause 252.204-7012 (Reference (al)) The clause requires a company to safeguard CDI, as defined in the Clause, and to report to the DoD the possible exfiltration, manipulation, or other loss or compromise of unclassified CDI; or other activities that allow unauthorized access to the contractor's unclassified information system on which unclassified CDI is resident or transiting. The company must submit the malware to DoD if the company is able to isolate it and send it safely. For more information on implementing this clause, also see "Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012," (Reference (ct)) released by the Office of the Deputy Assistant Secretary of Defense for Systems Engineering.
	DoD Instruction 5205.13 (Reference (co)) - Establishes an approach for protecting unclassified DoD information transiting or residing on unclassified defense industrial base information systems and networks. - Increases DoD and defense industrial base situational awareness. - Establishes a DoD and defense industrial base collaborative information sharing environment. - DoD CIO manages the Defense Industrial Base Cyber Security/ Information Assurance Program. - Codified in Part 236 of Title 32, Code of Federal Regulations (Reference (cp)).
	E.O. 13691 (Reference (cq)) Encourages and promotes sharing of cybersecurity threat information within the private sector and between the private sector and government.
OPSEC	DoD Directive 5205.02E (Reference (cn)) Establishes process for identifying critical information and analyzing friendly actions attendant to military operations and other activities to: - Identify those actions that can be observed by adversary intelligence systems. - Determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk. - Select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.
Protection of IT and Information Systems	DoD Instruction 8500.01 (Reference (x)) Establishes a DoD cybersecurity program to protect and defend DoD information and information technology.
	DoD Instruction 8510.01 (Reference (bg)) Establishes the DoD decision process for managing cybersecurity risk to DoD information technology.

Table 2. Cybersecurity and Related Program Security Resources and Publications, Continued

Category	Title of Resource and Description
System Protection	DoDI 5200.39 (Reference (ai)) Provides policy and procedures for protecting CPI. CPI includes U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermine U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.
	DoDI 5200.44 (Reference (aj)) Establishes policy and procedures for managing supply chain risk. A supply chain is at risk when an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.
	Section 933 of the National Defense Authorization Act for Fiscal Year 2013, Public Law 112-239 (Reference (l)) Requires use of appropriate automated vulnerability analysis tools in computer software code during the entire life cycle, including during development, operational testing, operations and sustainment phases, and retirement.
	Section 937 of Public Law 113-66 (Reference (bj)) Requires the DoD to establish a joint federation of capabilities to support trusted defense system needs to ensure the security of software and hardware developed, maintained, and used by the DoD.
	DoD Instruction 8530.01 (Reference (cu)) Establishes policy and assigns responsibilities to protect the DoDIN against unauthorized activity, vulnerabilities, or threats.
	Joint Federated Assurance Center, chartered under Section 937 of Public law 113-66 (Reference (bj)) Federation of subject matter experts and capabilities to support program hardware and software assurance needs.
	National Cyber Range (NCR) The NCR is institutionally funded by AT&L Test Resource Management Center to provide cybersecurity T&E as a service to DoD Customers. The NCR provides secure facilities, computing resources, repeatable processes and skilled workforce as a service to Program Managers. The NCR Team helps the Program Manager plan and execute a wide range of event types including S&T experimentation, architectural evaluations, security control assessments, cooperative vulnerability, adversarial assessments, training and mission rehearsal. The NCR creates hi-fidelity, mission representative cyberspace environments and also facilitates the integration of cyberspace T&E infrastructure through partnerships with key stakeholders across DoD, the Department of Homeland Security, industry, and academia.

Table 2. Cybersecurity and Related Program Security Resources and Publications, Continued

Category	Title of Resource and Description
Threat Assessment and Integration	Defense Intelligence Agency Produces intelligence and counterintelligence assessments, to include assessment of supplier threats to acquisition programs providing critical weapons, information systems, or service capabilities, and system threat intelligence reports.
	Defense Security Service Provides cleared U.S. defense industry with information about foreign intelligence threats and ensures that cleared U.S. defense industry safeguards the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts.
	JAPEC Collaboration among the acquisition, intelligence, counterintelligence, law enforcement, and operations communities to prevent, mitigate, and respond to data loss.
Risk, Issue, and Opportunity Management	"Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs" (Reference (cv)) A guidance document that addresses the significant relationship between program success and effective risk management.
Cybersecurity T&E	DOT&E, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" (Reference (cs)) A guidance document that describes approaches for operational cybersecurity testing.
	"Department of Defense Cybersecurity Test and Evaluation Guidebook" (Reference (cr)) A guidance document that addresses planning, analysis, and implementation of cybersecurity T&E for chief developmental testers, lead DT&E organizations, operational test agencies, and the larger test community.

GLOSSARY

A complete Glossary of acquisition terms and common acquisition acronyms is maintained on the Defense Acquisition University website (Reference (ce)). The DAU Glossary (Reference (cf)) may be found at https://dap.dau.mil/glossary/Pages/Default.aspx.