



Department of Defense INSTRUCTION

NUMBER 5000.02T

January 7, 2015

Incorporating Change 9, November 19, 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 5000.88, "Engineering of Defense Systems"
<ul style="list-style-type: none"> • Enclosure 4. Developmental Test and Evaluation (DT&E) • Enclosure 5. Operational and Live Fire Test and Evaluation (OT&E and LFT&E) 	DoDI 5000.89, "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	<ul style="list-style-type: none"> • 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.

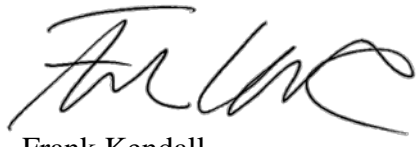
7. RELEASABILITY. **Cleared for public release**. This instruction is available on the Directives Division Website at <https://www.esd.whs.mil/DD/>.

8. SUMMARY OF CHANGE 9. This change removes:


a. Enclosure 3, which has been incorporated and cancelled by DoDI 5000.88 (Reference (df)).

b. Enclosures 4 and 5, which have been incorporated and cancelled by DoDI 5000.89 (Reference (dg)).


9. EFFECTIVE DATE. This instruction is effective January 7, 2015.



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



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 9	4
EFFECTIVE DATE	5
REFERENCES	8
ENCLOSURE 1: ACQUISITION PROGRAM CATEGORIES AND COMPLIANCE REQUIREMENTS	13
ENCLOSURE 2: PROGRAM MANAGEMENT	14
ENCLOSURE 3: SYSTEMS ENGINEERING	15
ENCLOSURE 4: DEVELOPMENTAL TEST AND EVALUATION (DT&E)	16
ENCLOSURE 5: OPERATIONAL AND LIVE FIRE TEST AND EVALUATION	17
ENCLOSURE 6: LIFE-CYCLE SUSTAINMENT	18
ENCLOSURE 7: HUMAN SYSTEMS INTEGRATION (HSI)	19
PURPOSE	19
GENERAL	19
HSI PLANNING	19
Human Factors Engineering	19
Personnel	19
Habitability	19
Manpower	20
Training	20
Safety and Occupational Health	20
Force Protection and Survivability	20

ENCLOSURE 8: AFFORDABILITY ANALYSIS AND INVESTMENT CONSTRAINTS.....	21
ENCLOSURE 9: ANALYSIS OF ALTERNATIVES (AOA).....	22
ENCLOSURE 10: COST ESTIMATING AND REPORTING	23
ENCLOSURE 11: REQUIREMENTS APPLICABLE TO ALL PROGRAMS CONTAINING INFORMATION TECHNOLOGY (IT).....	24
ENCLOSURE 12: URGENT CAPABILITY ACQUISITION	25
ENCLOSURE 13: CYBERSECURITY IN THE DEFENSE ACQUISITION SYSTEM.....	26
PROGRAM MANAGER RESPONSIBILITIES	26
Program Information.....	26
Organizations and Personnel.....	26
Enabling Networks.....	26
Systems, Enabling Systems, and Supporting Systems.....	26
ACTIVITIES TO MITIGATE CYBERSECURITY RISKS.....	26
Safeguard Program Information Against Cyber-Attack	26
Design for Cyber Threat Environments.....	26
Manage Cybersecurity Impacts to Information Types and System Interfaces to the DoDIN	29
PROTECTION PLANNING	29
Systems Engineering Plan (SEP).....	29
PPP	29
TEMP	30
Risk Management Framework for DoD IT Security Plan and Cybersecurity Strategy	30
RESOURCES FOR EXECUTING CYBERSECURITY AND RELATED PROGRAM SECURITY ACTIVITIES	30
GLOSSARY	34
TABLES	
1. Cybersecurity and Related Program Security Resources and Publications	31

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 amended¹
- (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 edition²
- (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, 2016³
- (u) Defense Intelligence Agency Instruction 5000.002, “Intelligence Threat Support for Major Defense Acquisition Programs,” September 19, 2016⁴
- (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/intelldocs/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 amended⁵
- (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, 2008⁶
- (as) Intelligence Community Policy Guidance 801.1, “Acquisition,” July 12, 2007⁷
- (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 version⁸
- (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 Website¹⁰
- (cf) Defense Acquisition University Glossary¹¹
- (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, 2016¹²
- (ci) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, “Change to Major Defense Acquisition Program Milestone B Requirements,” January 31, 2016¹³
- (cj) Integrated Program Management Report Implementation Guide, February 5, 2016¹⁴
- (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
- (df) DoD Instruction 5000.88, "Engineering of Defense Systems," 11/, 2020
- (dg) DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020

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

Enclosure 3 was removed through formal coordination and approval of Reference (df); necessary information can be found in that issuance.

ENCLOSURE 4

DEVELOPMENTAL TEST AND EVALUATION (DT&E)

Enclosure 4 was removed through formal coordination and approval of Reference (dg); necessary information can be found in that issuance.

ENCLOSURE 5

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

Enclosure 5 was removed through formal coordination and approval of Reference (dg); necessary information can be found in that issuance.

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) Developmental Testing

1. Cooperative Vulnerability Identification. 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.

2. Adversarial Cybersecurity DT&E. 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) Operational Testing. 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.

1. Cooperative Vulnerability and Penetration Assessment. 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 1 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 1. Cybersecurity and Related Program Security Resources and Publications

Category	
Information Protection	<p>FAR Clause 52.204-2 (Reference (ak))</p> <p>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.</p>
Protection of Information on Networks	<p>FAR Clause 52.204-21 (Reference (ak))</p> <p>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.</p>
	<p>DFARS Clause 252.204-7012 (Reference (al))</p> <p>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.</p> <p>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.</p>
	<p>DoD Instruction 5205.13 (Reference (co))</p> <ul style="list-style-type: none"> - 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)).
	<p>E.O. 13691 (Reference (cq))</p> <p>Encourages and promotes sharing of cybersecurity threat information within the private sector and between the private sector and government.</p>
OPSEC	<p>DoD Directive 5205.02E (Reference (cn))</p> <p>Establishes process for identifying critical information and analyzing friendly actions attendant to military operations and other activities to:</p> <ul style="list-style-type: none"> - 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	<p>DoD Instruction 8500.01 (Reference (x))</p> <p>Establishes a DoD cybersecurity program to protect and defend DoD information and information technology.</p>
	<p>DoD Instruction 8510.01 (Reference (bg))</p> <p>Establishes the DoD decision process for managing cybersecurity risk to DoD information technology.</p>

Table 1. Cybersecurity and Related Program Security Resources and Publications, Continued

Category	Title of Resource and Description
System Protection	<p>DoDI 5200.39 (Reference (ai))</p> <p>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.</p>
	<p>DoDI 5200.44 (Reference (aj))</p> <p>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.</p>
	<p>Section 933 of the National Defense Authorization Act for Fiscal Year 2013, Public Law 112-239 (Reference (l))</p> <p>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.</p>
	<p>Section 937 of Public Law 113-66 (Reference (bj))</p> <p>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.</p>
	<p>DoD Instruction 8530.01 (Reference (cu))</p> <p>Establishes policy and assigns responsibilities to protect the DoDIN against unauthorized activity, vulnerabilities, or threats.</p>
	<p>Joint Federated Assurance Center, chartered under Section 937 of Public law 113-66 (Reference (bj))</p> <p>Federation of subject matter experts and capabilities to support program hardware and software assurance needs.</p>
	<p>National Cyber Range (NCR)</p> <p>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.</p>

Table 1. Cybersecurity and Related Program Security Resources and Publications, Continued

Category	Title of Resource and Description
Threat Assessment and Integration	<p>Defense Intelligence Agency</p> <p>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.</p>
	<p>Defense Security Service</p> <p>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.</p>
	<p>JAPEC</p> <p>Collaboration among the acquisition, intelligence, counterintelligence, law enforcement, and operations communities to prevent, mitigate, and respond to data loss.</p>
Risk, Issue, and Opportunity Management	<p>“Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs” (Reference (cv))</p> <p>A guidance document that addresses the significant relationship between program success and effective risk management.</p>
Cybersecurity T&E	<p>DOT&E, “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs” (Reference (cs))</p> <p>A guidance document that describes approaches for operational cybersecurity testing.</p>
	<p>“Department of Defense Cybersecurity Test and Evaluation Guidebook” (Reference (cr))</p> <p>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.</p>

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>.