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
(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 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

Table 1. Cybersecurity and Related Program Security Resources and Publications

Category	
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 1. 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 1. 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.