THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

January 11, 2017

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-type Memorandum (DTM) 17-001 – Cybersecurity in the Defense Acquisition System

References: See Attachment 1.

Purpose. In accordance with the authority in DoD Directive (DoDD) 5134.01, this DTM:

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

- This DTM is effective January 11, 2017; it must be incorporated into DoD Instruction (DoDI) 5000.02. This DTM will expire January 11, 2018.

Applicability. This DTM 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 the 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 DTM as the "DoD Components").

Policy. It is DoD policy that:

- Cybersecurity be fully considered and implemented in all aspects of acquisition programs across the life cycle.

- Responsibility for cybersecurity extends to all members of the acquisition workforce.

Procedures. See Attachment 2.

Releasability. **Cleared for public release**. This DTM is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

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

Attachments:
As stated

## ATTACHMENT 1

## REFERENCES

Code of Federal Regulations, Title 32, Part 236

Defense Federal Acquisition Regulation Supplement, current edition

DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005, as amended

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

DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015

DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015

DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, as amended

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

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

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

Federal Acquisition Regulation, current edition

Public Law 112-239, Section 933, "National Defense Authorization Act for Fiscal Year 2013," January 2, 2013

Public Law 113-66, Section 937, "National Defense Authorization Act for Fiscal Year 2014," December 26, 2013

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

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

Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation, "Department of Defense Cybersecurity Test and Evaluation Guidebook," July 1, 2015

Director, Operational Test and Evaluation, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," August 1, 2014

# ATTACHMENT 2

## CYBERSECURITY IN THE DEFENSE ACQUISITION SYSTEM

### 1. INTRODUCTION

a. Cyber Impact on Defense Acquisition

(1) Cybersecurity is a requirement for all DoD programs. DoD program offices, systems, and networks, and supporting contractor facilities and activities, are at risk of cyber-attacks by state and non-state threat actors. Malicious activity by threat actors includes remote unauthorized activity against DoD to:

(a) Exfiltrate operational and classified data to compromise or disrupt critical DoD missions.

(b) Exfiltrate intellectual property, designs, or technical documentation to weaken DoD technological and military advantage.

(c) Insert compromised hardware or software to disrupt or degrade system performance.

(d) Subvert or compromise DoD networks, systems, support infrastructure, and employees through malicious actions.

(2) Responsibility for cybersecurity extends beyond network operators, software developers, and chief information officers, to every member of the acquisition workforce. Attention must be paid to cybersecurity at all acquisition category levels and all classification levels, including unclassified, throughout the entire life cycle. This includes systems that reside on networks and stand alone systems that are not persistently connected to networks during tactical and strategic operations.

b. Program Manager (PMs) Responsibilities. PMs, 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. PMs will pay particular attention to the following areas where a cybersecurity breach or failure would jeopardize military technological advantage or functionality:

(1) Program Information. This includes, but is not limited to:

(a) 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.

(b) 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.

(2) 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.

(3) 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.

(4) 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. CYBERSECURITY RISKS. Cyber vulnerabilities provide potential exploitation points for adversaries to steal, alter, or destroy system functionality, information, or technology they seek. PMs will pay particular attention to the program and system elements that are vulnerable and can be exposed to targeting. At a minimum, the PM’s technical risk and opportunity management will consider:

a. Government Program Organization. Poor cybersecurity practices, untrained personnel, undetected malicious insiders, insufficient or incorrect classification of information and dissemination handling control, and inadequate information network security can be used by threat actors to gain program and system knowledge.

b. Contractor Organizations and Environments. Contractor facilities, including design, development, and production environments, networks, supply chains, and personnel, can be used by threat actors as cyber pathways to access government program organizations or fielded systems to steal, alter, or destroy system functionality, information, or technology.

c. Software and Hardware. Software, including firmware, and microelectronics used in the system or incorporated into spares can be deliberately compromised while in the supply chain with the intent to use these compromises for cyber-attacks to trigger future system failures. Undiscovered weaknesses or flaws in system elements containing software or microelectronics, including spares, can provide the foundation for threat actors to defeat fielded systems through cyber-attacks.

d. System Interfaces. Poorly configured, inadequately maintained, undocumented, or unprotected network and system interfaces can be used by threat actors to gain unauthorized system access or deliver cyber-attacks in the form of malicious software or content.

e. Enabling and Support Equipment, Systems, and Facilities. Test, certification, maintenance, design, development, manufacturing, or training systems, equipment, and facilities can be used by threat actors to gain access to system functionality, information or technology for cyber-attacks.

f. Fielded Systems. Degradation of the cybersecurity configuration or poor cyber hygiene conditions can expose system functionality to unauthorized access that threat actors can potentially exploit to gain access to system functionality. Battlefield loss can expose critical program information (CPI) to cyber threats.

3. ACTIVITIES TO MITIGATE CYBERSECURITY RISKS. PMs 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. PMs will:

(1) Safeguard digitized information, starting with the application of appropriate classification and marking guidance for all program data, with a key focus on classified information and unclassified covered defense information (CDI), which includes unclassified controlled technical information. Programs that contain classified information can contain unclassified CDI, and the compilation of CDI can become classified. PMs will assess the impact of the exposure of the unclassified program information that will be placed on unclassified networks, including information that is contained in solicitations, technical publications, and associated research and technology efforts.

(2) Promote a strong culture of cybersecurity awareness and behavior in program offices and among contractors. This includes practicing need to know, good network security, and OPSEC, as described in DoDD 5205.02E, whenever and wherever digital information and communications are concerned.

(3) Ensure Federal Acquisition Regulation (FAR) Clause 52.204-2 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.

(4) 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.

(5) Ensure Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 is included in all solicitations and contracts, including solicitations and contracts using FAR part 12 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.

(6) 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.

(7) Encourage contractor and industry participation in public-private information sharing activities, such as those described in DoDIs 5205.13 and 8500.01, and codified in Part 236 of Title 32, Code of Federal Regulations. or those developed under Executive Order (E.O.) 13691.

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

(1) Derive cybersecurity and other system requirements into system performance specifications and product support needs as follows:

(a) Use the draft or validated capability development document (CDD) or equivalent capability requirements document, the concept of operations, the operational mode summary/mission profiles, and the assessed threats to the military capability provided by the Defense Intelligence Agency (DIA) or DoD Component intelligence and counterintelligence activities to inform requirements derivation activities.

(b) Ensure key performance parameters and attributes establish system survivability and sustainment measures, and may establish information system security measures, such as cryptography and key distribution, based on confidentiality, integrity and availability needs.

(c) Use requirements derivation methods, such as system modeling and analysis, security use and abuse or misuse cases, criticality analysis, and vulnerability analysis to determine cybersecurity requirements that are sufficient to minimize vulnerabilities introduced by design, implementation, system interfaces and access points.

(2) Allocate cybersecurity and related system security requirements to the system architecture and design, and assess for vulnerabilities.

(a) The system architecture and design will address, at a minimum, how the system:

1. Manages access to and use of the system and system resources.

2. Is structured to protect and preserve system functions or resources, (e.g., through segmentation, separation, isolation, or partitioning).

3. Maintains priority system functions under adverse conditions.

4. Is configured to minimize exposure of vulnerabilities that could impact the mission, including through techniques such as design choice, component choice, security technical implementation guides and patch management in the development environment (including integration and T&E), in production and throughout sustainment.

5. Monitors, detects, and responds to security anomalies.

6. Interfaces with DoD Information Network (DoDIN) or other external security services.

(b) 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 3.b.(2)(a), 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.

(c) Apply DoDIs 8500.01 and 8510.01 in accordance with DoD Component implementation and governance procedures. PMs 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. PMs 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) Ensure cybersecurity and related system security requirements, design characteristics, and verification methods to demonstrate the achievement of those requirements are included in the technical baseline and maintain bi-directional traceability among requirements throughout the system life cycle.

(4) Include cybersecurity and related system security in the conduct of technical risk management activities and change management processes to address risk identification, analysis, mitigation planning, mitigation implementation, and tracking. Use evolving program and system threats to inform operational impacts. The goal is to mitigate risks that could have an 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 cybersecurity cost and schedule implications.

(5) Use evolving program and system threat assessments to continuously assess cybersecurity risks to the program and system.

(6) Identify and protect CPI, capabilities that contribute to the warfighters' technical advantage, throughout the life cycle in accordance with DoDI 5200.39. PMs will:

(a) Identify and implement AT and exportability features as appropriate to protect CPI in U.S. systems when outside of U.S. control in accordance with DoDI 5200.39.

(b) Coordinate with the applicable DoD Component office of primary responsibility for AT, for programs with CPI. Submit an AT concept before Milestone A and AT plans before Milestones B and C; the DoD Executive Agent for AT must concur with the concept and plans, and the Milestone Decision Authority must approve the concept and plans as an element of the Program Protection Plan (PPP) in accordance with Enclosure 3 of DoDI 5000.02 and DoDI 5200.39.

(7) Use trusted suppliers or appropriate SCRM countermeasures for system elements that perform mission-critical functions. Cyber protection measures for mission-critical functions and critical components must, at a minimum, include software assurance, hardware assurance, procurement strategies, and anti-counterfeit practices in accordance with DoDI 5200.44.

(8) Use validated cybersecurity solutions, products, and services when available and cost effective.

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

(10) Implement a cyber system vulnerability discovery and remediation process that spans research, development, production, and sustainment and integrates activities by both the government and contractors.

(11) Request assistance, when appropriate, from the Joint Federated Assurance Center, established in accordance with Section 937 of Public Law 113-66, to support software and hardware assurance requirements.

(12) Incorporate automated software vulnerability analysis tools throughout the life cycle to evaluate software vulnerabilities, as required by Section 933 of Public Law 112-239. When appropriate, use software vulnerability analysis enterprise licenses provided by the Joint Federated Assurance Center.

(13) 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 Cybersecurity T&E Guidebook and the Director of Operational Test and Evaluation "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," 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 Working Integrated Product Team to plan, as described in Paragraph 3.b.(2), and conduct cybersecurity T&E, as described in Paragraphs 3.b.(13)(a) and 3.b.(13)(b), 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. PMs 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 PM. 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 Director of Operational Test and Evaluation 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.

(14) Ensure that cybersecurity and system security requirements are incorporated in contracts.

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. PMs 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 PM 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.

d. Protect the System Against Cyber Attacks From Enabling and Supporting Systems. PMs will:

(1) Identify all system interfaces to all enabling and supporting systems and assess cybersecurity vulnerabilities. PMs will review vulnerabilities introduced by enabling and supporting systems and support activities, including engineering, simulation, and test tools and environments, third party certification and assessment activities, logistics, maintenance and training support activities, and all interoperable or ancillary equipment which the system operates or interfaces.

(2) Use threat intelligence from DIA, DoD Component intelligence and counterintelligence activities, the Defense Security Service, and the JAPEC to assess the

trustworthiness of third party service providers and environments, (e.g., training, testing, logistics, or certification).

e. Protect Fielded Systems. Cybersecurity and related system security measures implemented throughout the system development effort do not ensure security is maintained throughout operations. Once systems are fielded, they become exposed to a changing cyber threat environment and potentially more vulnerabilities. Planning for maintaining the cybersecurity of the system must be considered early and throughout the life cycle. PMs will:

(1) Plan for and implement effective software configuration updates and software management, to include software patch management during sustainment to mitigate newly discovered vulnerabilities. For high impact mission critical functions as established in accordance with DoDI 5200.44 consider having a user representative as part of the software configuration management risk acceptance process.

(2) Plan, define, and document roles and responsibilities in the appropriate logistics documentation, (e.g., software support plan, operational technical manuals, planned maintenance support), for monitoring, maintaining, and reassessing cybersecurity and related program security risks as it relates to in-service usage, problem reports, configuration management, patch management, plan for Diminishing Manufacturing Sources and Materiel Shortages, and SCRM, to include counterfeits of critical components. This must include plans for coordinating cyber threat intelligence support throughout operations to ensure cybersecurity and related program security risk management accounts for changes to threats.

(3) Conduct periodic reassessments of cyber vulnerabilities to the system and support systems. These reassessments must be conducted, at a minimum, for any engineering modifications or technology refreshes. Technical and process mitigations will be incorporated into engineering and logistics documentation, and related solicitations and contracts.

(4) Ensure program and system information are protected and cyber vulnerabilities introduced by depot and other sustainment activities are minimized.

(5) Ensure identified CPI is protected from cyber-attack through disposal.

f. Independent Acquisition, Engineering, and Technical Assessments. For acquisition category I programs, DoD Component heads will conduct independent assessments of system designs and interfaces for cyber vulnerabilities. The results must inform technical baselines, and T&E plans and procedures.

## 4. PROTECTION PLANNING

a. Systems Engineering Plan (SEP). PMs will ensure the SEP, developed in accordance with Enclosure 3 of DoDI 5000.02, 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 DoDI 5000.02, PMs 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 Milestone Decision Authority approval at each milestone review, beginning with Milestone A.

(1) PMs 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 PM 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 DoDI 5000.02, 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, PMs will prepare plans and strategies in accordance with DoDI 8510.01 and applicable DoD Component issuances.

## 5. PROGRAM MANAGEMENT AND COMPONENT ACTIONS TO IMPLEMENT CYBERSECURITY AND RELATED PROGRAM SECURITY ACROSS THE MATERIEL LIFE CYCLE

a. Prior to Materiel Development Decisions. Research, development, test, and evaluation (RDT&E) organizations and PMs will:

(1) Request cyber threat information from DIA or DoD Component intelligence and counterintelligence activities and use threat assessments to inform cyber protection planning.

(2) Protect digitized information from adversary targeting during basic and applied research, advanced technology development (including technology demonstrations and prototyping) and capabilities-based assessments.

(3) Identify CPI from science and technology (S&T) programs and initiate life-cycle cyber protection measures.

(4) Support the requirements community in the formulation of cybersecurity performance and affordability parameters and the identification of security-relevant critical intelligence parameters, and ensure key technical requirements are measurable and testable.

(5) Initiate all aspects of cyber related program protection planning, (e.g., counterintelligence, information security classification, and OPSEC).

b. Materiel Solutions Analysis (MSA) Phase. During the MSA phase, RDT&E organizations and PMs will:

(1) Request information on cyber threats targeting program information and the system from DIA or DoD Component intelligence/counterintelligence activities and use updated threat assessments to inform the Analysis of Alternatives (AoA), early systems engineering analyses, selection of a preferred materiel solution and development of the draft CDD (or equivalent requirements document).

(2) Protect S&T, program, and system information from adversary cyber threat targeting during the MSA phase, including AoA, analyses and program such as formulation of the acquisition strategy and in requests for information or proposals.

(3) Manage technical risks and opportunities to include cybersecurity and related program security across the life cycle and informs all aspects of program security and cybersecurity planning.

(4) Establish program and system cybersecurity and related program security metrics and implement an enduring monitoring and assessment capability.

(5) Identify CPI and initiate life cycle protection measures.

(6) Evaluate materiel solution alternatives for cybersecurity requirements, including but not limited to interfaces, performance, and sustainability, to support the AoA.

(7) Support the formulation of cybersecurity performance and affordability parameters and the identification of security-relevant critical intelligence parameters for the draft CDD.

(8) Update and integrate all cybersecurity related aspects of the program protection planning, to include but not limited to information security, OPSEC and life cycle support.

(9) Define system cybersecurity entrance and exit criteria for all technical reviews, and document in the SEP along with related system security metrics for the program and system.

(10) Develop a cybersecurity T&E methodology based on derived system requirements and draft system performance specifications. Compile and analyze the system security requirements, identifying the data needed to support engineering, risk management and acquisition decisions. Ensure the key system elements and interfaces identified through

criticality and vulnerability analysis are tested during T&E. Document T&E planning in the TEMP. Identify the cybersecurity T&E resources, (e.g., cyber ranges) for each T&E activity.

(11) For programs requiring a DoD IT Authorization to Operate, in accordance with DoDIs 8500.01 and 8510.01 in accordance with applicable DoD Component issuances, coordinate authorization planning in accordance with DoD Component implementation and governance procedures.

c. Technology Maturation and Risk Reduction (TMRR) Phase. During the TMRR phase, PMs will:

(1) Request cyber threat information from DIA or DoD Component intelligence and counterintelligence activities and make use of updated cyber threat assessments to inform systems engineering trade-off analyses to support requirements, investment, and acquisition decisions. The analysis results should be reassessed over the life cycle as system requirements, design, manufacturing, test, and logistics activities evolve and mature.

(2) Protect digitized program and system information, CPI, and other system elements from adversary targeting during TMRR activities including system definition, design and test, contracting, and competitive prototyping.

(3) Analyze system requirements and design to ensure the system as described in the functional and allocated baselines meets cybersecurity performance requirements for operations in applicable cyber threat environments.

(4) Establish cybersecurity-relevant technical performance parameters and update the technical review entrance and exit criteria in the SEP.

(5) Update and integrate all cyber related aspects of the program protection planning, to include but not limited to information security, OPSEC, and life-cycle support. For T&E, understand the cyber-attack surfaces and refine the T&E planning and activities for cybersecurity; include updates in the Milestone B TEMP. Identify the cybersecurity T&E resources, such as cyber ranges, for each T&E activity. Ensure that an adversarial cybersecurity DT&E event is planned in a mission context.

(6) Incorporate cyber protection of program and system information, CPI, system elements (e.g., hardware assurance and software assurance) and cybersecurity performance requirements in the development RFP.

(7) Employ need to know principles and criteria when structuring contracting activities to minimize release of digitized program and system information. Include system security evaluation factors and subfactors that are tied to significant RFP security requirements and objectives that will have an impact on the source selection decision and are expected to be discriminators, (e.g., implementing safeguarding information on the contractors unclassified owned and operated network).

d. Engineering and Manufacturing Development (EMD) Phase. During the EMD phase, PMs will:

(1) Request cyber threat information on threats targeting program information and the system from DIA or DoD Component intelligence and counterintelligence activities and use updated threat assessments to inform development of the detailed design, T&E criteria, system-level security risk, and assessment of readiness to begin production and deployment.

(2) Protect digitized program, system, and test information, CPI, and system elements from adversary targeting during design, test, and manufacturing and production readiness.

(3) Update cybersecurity and system security entrance and exit criteria for all technical reviews and document in the SEP.

(4) Update and integrate all aspects of the program protection planning, to include but not limited to information security, OPSEC, and life-cycle support.

(5) Conduct cybersecurity vulnerability and penetration testing and evaluation at the component, subsystem, interface, and integration levels in order to verify system requirements are met, and use results to inform the engineering activities, including technical risk and opportunity management.

(6) Incorporate recommendations from security T&E of EMD test articles and ensure the system as described in the production baseline is configured to established cybersecurity parameters and satisfies performance requirements for operations in applicable cyber threat environments. Ensure an adversarial cybersecurity DT&E event is conducted to evaluate the system's cybersecurity performance within a mission context. Use realistic threat exploitation techniques in representative operating environments and scenarios.

e. Production and Deployment Phase. During the production and deployment phase, PMs will:

(1) Request cyber threat information on threats targeting program information and the system from DIA or DoD Component intelligence/counterintelligence activities and make use of updated threat assessments to inform production and deployment activities such as, manufacturing, training spares.

(2) Protect digitized program and system information, CPI, and the system from adversary targeting during initial production, operational T&E and initial fielding.

(3) Ensure the final product baseline includes cybersecurity design and configuration.

(4) Ensure system documentation addresses how to operate the system securely and how to manage and preserve the system security configuration.

(5) Ensure the system is deployed in a secure configuration.

(6) Update all aspects of program protection planning for the program and the system as cyber threats and the system evolve.

(7) Test the system for cybersecurity vulnerabilities using realistic threat exploitation techniques in an operational environment and remediate as appropriate.

(a) Coordinate with the appropriate operational test agency to support the execution of a cybersecurity cooperative vulnerability and penetration assessment. This assessment must include the enumeration of all significant vulnerabilities and the identification of exploits which may be employed against those vulnerabilities.

(b) Coordinate with the appropriate operational test agency to support the execution of a cybersecurity adversarial assessment, following the cooperative vulnerability and penetration assessment, to examine and characterize the operational impact of the vulnerabilities and exploits previously identified.

f. Operations and Support Phase. During the operations and support phase, PMs will:

(1) Request cyber threat information on threats targeting program information and systems in operation from DIA or DoD Component intelligence and counterintelligence activities and make use of updated threat assessments to inform impact to operational systems, technology refresh and disposal plans.

(2) Protect digitized program and system information, CPI, and system from adversary targeting during fielding and sustainment activities such as maintenance, training and operational exercises.

(3) Protect support systems and system spares from impairing cyber threats mission critical system functions.

(4) Respond to vulnerability alerts and apply security patches promptly.

(5) Periodically assess cybersecurity and other program security risks during system upgrades (e.g., technology refresh, modifications, engineering changes or future increments).

(6) Update all aspects of program protection planning for the program and the system as cyber threats and systems evolve.

(7) Before system disposal, remove all CPI and system data.

6. RESOURCES FOR EXECUTING CYBERSECURITY AND RELATED PROGRAM SECURITY ACTIVITIES. Table 1 lists and describes various resources and publications available for the PM to use in executing cybersecurity and related program security procedures detailed in this attachment.

Table 1. Cybersecurity and Related Program Security Resources and Publications

| Category | Title of Resource and Description |
|---|---|
| Information Protection | *FAR Clause 52.204-2*<br>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*<br>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*<br>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.<br>For more information on implementing this clause, also see Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012, released by the Office of the Deputy Assistant Secretary of Defense for Systems Engineering. |
| | *DoD Instruction 5205.13*<br>- Establishes an approach for protecting unclassified DoD information transiting or residing on unclassified defense industrial base information systems and networks.<br>- Increases DoD and defense industrial base situational awareness.<br>- Establishes a DoD and defense industrial base collaborative information sharing environment.<br>- DoD Chief Information Officer manages the Defense Industrial Base Cyber Security/ Information Assurance Program.<br>- Codified in Part 236 of Title 32, Code of Federal Regulations. |
| | *E.O. 13691*<br>Encourages and promotes sharing of cybersecurity threat information within the private sector and between the private sector and government. |
| OPSEC | *DoD Directive 5205.02E*<br>Establishes process for identifying critical information and analyzing friendly actions attendant to military operations and other activities to:<br>- Identify those actions that can be observed by adversary intelligence systems.<br>- 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.<br>- 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*<br>Establishes a DoD cybersecurity program to protect and defend DoD information and information technology |
| | *DoD Instruction 8510.01*<br>Establishes the DoD decision process for managing cybersecurity risk to DoD information technology. |
| System Protection | *DoDI 5200.39*<br>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*<br>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*<br>Requires use of appropriate automated vulnerability analysis tools in computer software code during the entire |

Table 1. Cybersecurity and Related Program Security Resources and Publications

| Category | Title of Resource and Description |
|---|---|
| | life cycle, including during development, operational testing, operations and sustainment phases, and retirement. |
| | *Section 937 of Public Law 113-66*<br>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 8530.10*<br>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*<br>Federation of subject matter experts and capabilities to support program hardware and software assurance needs. |
| | *National Cyber Range (NCR)*<br>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 PMs. The NCR Team helps the PM 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. |
| Threat Assessment and Integration | *Defense Intelligence Agency*<br>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*<br>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. |
| Threat Assessment and Integration | *JAPEC*<br>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*<br>A guidance document that addresses the significant relationship between program success and effective risk management. |
| Cybersecurity T&E | *Director of Operational Test and Evaluation, Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs*<br>A guidance document that describes approaches for operational cybersecurity testing. |
| | *Department of Defense Cybersecurity Test and Evaluation Guidebook*<br>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

### ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| AoA | analysis of alternatives |
| AT | anti-tamper |
| CDD | capability development document |
| CDI | covered defense information |
| CPI | critical program information |
| DFARS | Defense Federal Acquisition Regulation Supplement |
| DIA | Defense Intelligence Agency |
| DoDD | DoD directive |
| DoDI | DoD instruction |
| DoDIN | DoD information network |
| DT&E | developmental test and evaluation |
| EMD | Engineering and Manufacturing Development |
| E.O. | Executive Order |
| FAR | Federal Acquisition Regulation |
| IT | information technology |
| JAPEC | Joint Acquisition Protection and Exploitation Cell |
| MSA | materiel solution analysis |
| NCR | National Cyber Range |
| NSA/CSS | National Security Agency/Central Security Service |
| OPSEC | operations security |
| PM | program manager |
| PPP | Program Protection Plan |
| RDT&E | research, development, test and evaluation |
| RFP | request for proposal |
| SCRM | supply chain risk management |
| SEP | Systems Engineering Plan |
| S&T | science and technology |
| TEMP | Test and Evaluation Master Plan |
| TMRR | Technology Maturation and Risk Reduction |
| T&E | test and evaluation |

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu