DoD Instruction 3020.45

Mission Assurance Construct

Originating Component:	Office of the Under Secretary of Defense for Policy
Effective: **Change 1 Effective:**	August 14, 2018 May 2, 2022
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues:	DoD Instruction 3020.45, “Defense Critical Infrastructure Program (DCIP) Implementation” April 21, 2008, as amended
Incorporates and Cancels:	DoD Manual 3020.45, Volume 1, “Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP),” October 24, 2008, as amended DoD Manual S-3020.45, Volume 4, “Defense Critical Infrastructure Program (DCIP): Defense Critical Asset (DCA) Nomination and Submission Process,” March 20, 2009
Cancels:	DoD Manual 3020.45 Volume 2, “Defense Critical Infrastructure Program (DCIP): DCIP Remediation Planning,” October 28, 2008, as amended DoD Manual 3020.45 Volume 5, “Defense Critical Infrastructure Program (DCIP): Execution Timeline,” May 24, 2010, as amended
Approved by: **Change 1 Approved by:**	John C. Rood, Under Secretary of Defense for Policy Colin H. Kahl, Under Secretary of Defense for Policy

Purpose: In accordance with the authority in DoD Directives (DoDDs) 5111.01 and 3020.40, this issuance establishes policy, assigns responsibilities, and provides procedures for the establishment and execution of the Mission Assurance (MA) Construct. It also establishes the minimum requirements for risk management of non-DoD owned defense critical infrastructure (DCI) and rescinds the DoD Mission Assurance Implementation Framework from October 7, 2013.

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to the OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (CCMDs), 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 issuance as the "DoD Components").

1.2. POLICY.

a. DoD establishes the MA Construct as the DoD-wide process to identify, assess, manage, and monitor the risks to strategic missions.

b. The MA Construct will support strategic guidance priorities by providing the Secretary of Defense (SecDef) and Deputy Secretary of Defense (DepSecDef) with recommendations to accept, mitigate, or remediate strategic risks. Risks include those to U.S. interests identified in the National Defense Strategy and military risks identified in the National Military Strategy through the Planning, Programming, Budgeting, and Execution (PPBE), acquisition, and Joint Capabilities Integration and Development System (JCIDS) processes.

c. Protection programs support the MA Construct by providing a framework that enables commanders to integrate, synchronize, and adjust standards applicable to preserving the effectiveness and survivability of mission assets, systems, and personnel.

1.3. INFORMATION COLLECTIONS. The MA Construct and system of record referred to in Paragraph 3.1. of this issuance does not require licensing with a report control symbol in accordance with Paragraph 1(b)(8) of Volume 1 of Enclosure 3 to DoD Manual 8910.01.

1.4. SUMMARY OF CHANGE 1. The changes to this issuance:

a. Document the changes to the MA Construct's responsibilities and the implementation sections on assessments and risk management:

(1) To improve intelligence, counterintelligence, and security support to MA to enhance understanding of threats and risks from near-peer adversaries in the competition-to-conflict continuum.

(2) To enhance the assessment process to identify more effectively vulnerabilities that are exploitable by near-peer adversary capabilities, with increased focus on the areas of cyber and emerging technologies.

(3) To reduce the timeline for risk-management decisions and subsequent implementation with a final risk decision within 1 year of on-site assessment completion.

(4) By integrating the mission-relevant terrain in cyberspace (MRT-C) analysis with MA.

b. Clarify policy to address questions and conflicts identified during initial implementation of the MA Construct.

c. Administratively update organizational titles and references for currency and accuracy.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). In addition to the responsibilities in Paragraph 2.19., the USD(P):

a. Advises the SecDef and DepSecDef on:

(1) Strategic mission risk or protection issues identified or addressed through MA.

(2) Major MA resource allocations and investments during the yearly Defense Planning Guidance development process, including mission assurance coordination board (MACB) recommendations on whether to initiate, continue, modify, or terminate individual investments.

(3) MA-related inputs to the Secretary's risk mitigation plan that accompanies the Chairman's Risk Assessment to Congress and provides the OSD response to risk issues raised by the Chairman.

b. Integrates MA objectives into DoD strategies, strategic guidance, plans, and policies including international security strategies, alliance treaties, and defense partnership agreements, as required.

c. Establishes policy for performing defense industrial base (DIB) sector-specific agency responsibilities identified in Presidential Policy Directive-21 and the National Infrastructure Protection Plan (NIPP), and aligns these activities with the MA Construct.

d. Advises the SecDef on force posture decisions and high-demand, low-density critical capability allocations in a globally integrated environment and execution of globally integrated operations.

2.2. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND HEMISPHERIC AFFAIRS (ASD(HD&HA)). Under the authority, direction, and control of the USD(P), the ASD(HD&HA):

a. Serves as the original classification authority (OCA) for the DCI line of effort under MA.

b. Co-chairs the MA Executive Steering Group (MA ESG) with the Director, Joint Staff, to:

(1) Provide recommendations of defense critical assets (DCAs) to the SecDef, based upon CJCS nominations and input from the appropriate Principal Staff Assistants.

(2) Examine strategic risk issues and provide risk recommendations on strategic redundancy and resiliency to the SecDef.

c. As the Principal Cyber Advisor, aligns Principal Cyber Advisor activities with MA by:

(1) Establishing prioritization guidance for cybersecurity and cyber defense capabilities, in coordination with DoD Chief Information Officer (CIO), and provides these to the Commander, United States Cyber Command (CDRUSCYBERCOM).

(2) Partnering with allied and partner nations to execute cyber-related MA activities.

d. Provides MA system of record requirements corresponding to the needs of the SecDef, DepSecDef, and USD(P) to the Director, Defense Threat Reduction Agency (DTRA), for incorporation into system design and development.

e. Provides recommendations concerning vulnerability remediation funding in the PPBE process, in support of DoD-owned assets.

2.3. ASSISTANT SECRETARY OF DEFENSE FOR STRATEGY, PLANS, AND CAPABILITIES. Under the authority, direction, and control of the USD(P), the Assistant Secretary of Defense for Strategy, Plans, and Capabilities:

a. Advises DoD Components on the timelines for campaign plan, operational plan (OPLAN), and concept plan (CONPLAN) development or rewrites for synchronizing MA efforts.

b. Provides guidance for inclusion of mission mitigation plans (MMPs) in campaign plans, OPLANs, and CONPLANs.

c. Provides recommendations to DoD Components on high-demand, low-density critical capability allocations in a globally integrated environment and execution of globally integrated operations.

d. Ensures that task critical assets (TCAs) and their respective MRT-C and mission-relevant terrain in space are identified and recorded in OPLANs and CONPLANs to the maximum extent possible.

2.4. DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR DEFENSE CONTINUITY AND MISSION ASSURANCE (DASD(DC&MA)). Under the authority, direction, and control of the USD(P), the DASD(DC&MA):

a. Establishes an office of primary responsibility (OPR) to provide policy and oversight of MA and the DCI line of effort activities.

b. Co-chairs the MA Senior Steering Group (MA SSG) with the Vice Director, Joint Staff to:

(1) Coordinate with appropriate governance bodies and establish working groups to address risks to the Department's strategic missions and essential capabilities.

(2) Establish and oversee departmental-level MA priorities, including:

(a) Reviewing assessment results regarding DCAs and other MACB-prioritized DCI.

(b) Providing risk management analysis and remediation and mitigation courses of action (COAs) to the MA ESG for DCAs and other MACB-prioritized DCI.

(c) Monitoring execution of approved risk management plan (RMP) implementation.

(3) Address strategic concerns raised by MA-related programs and activities.

c. Synchronizes the DCI line of effort, antiterrorism (AT), DoD Force Protection Condition System, and continuity of operations (COOP) with MA by ensuring each effort:

(1) Develops program standards and requirements to support the mission assurance assessment program (MAAP), provides these to the CJCS, and works with the CJCS to develop MAAP benchmarks for each program and activity.

(2) Reviews program-related risks discovered through the MAAP and updates policy and guidance to address systemic issues, when required.

(3) Provides MA system of record requirements to the Director, DTRA.

(4) Provides representation at the MA SSG for issues related to these portfolios.

(5) Updates security or protection standards for DCI and MA priorities, as applicable.

(6) Incorporates the principles of the MA Construct in guiding policies.

d. Develops a partnership strategy and mechanisms for addressing risk to non-DoD-owned infrastructure and critical capabilities in support of defense critical missions.

e. Designates, provides strategic direction and priorities, and supports MA centers of excellence to address key MA capabilities that benefit the entire DoD enterprise for functions such as:

(1) Mission analysis.

(2) Engineering and commercial infrastructure network and interdependency analysis, within appropriate legal limits.

(3) MA assessments (MAAs).

(4) MA system of record development and management.

(5) DIB supply chain network and related analysis.

(6) Data acquisition, sharing, and collaboration to improve threat analysis and prioritization of support to MAAs.

(7) Defense Information System Network (DISN) network and related analysis.

f. Ensures resourcing of the centers of excellence for MA and infrastructure analysis meets the strategic MA priority needs of the Department.

g. Identifies, in coordination with the CJCS, strategic issues for the MACB based upon DTRA and Service MAA results. Provides these strategic issues to MACB co-chairs for designation of lead DoD Components for each issue.

2.5. DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE INTEGRATION AND DEFENSE SUPPORT OF CIVIL AUTHORITIES. Under the authority, direction, and control of the USD(P), the Deputy Assistant Secretary of Defense for Homeland Defense Integration and Defense Support of Civil Authorities:

a. Synchronizes the chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) protection effort with MA by ensuring the CBRNE protection effort:

(1) Develops program standards and requirements to support the MAAP and provides these to the CJCS, and works with the CJCS to develop MAAP benchmarks for CBRNE protection.

(2) Reviews CBRNE protection-related risks discovered by the MAAP and updates policy and guidance to address systemic issues, when required.

(3) Provides MA system of record requirements to the Director, DTRA.

(4) Provides representation at the MA SSG for related issues.

(5) Updates CBRNE protection standards for DCI and MA priorities, as applicable.

(6) Incorporates the principles of the MA Construct in guiding policies.

b. Integrates MA objectives into homeland defense and Defense Support of Civil Authorities efforts, as required.

2.6. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT (USD(A&S)). In addition to the responsibilities in Paragraph 2.19., the USD(A&S):

a. Integrates emergency management (EM) activities with MA to:

(1) In accordance with DoD Instruction (DoDI) 4000.19, ensure support agreements account for DCI revealed by the MA identification process described in Section 3, when all parties meet necessary security requirements.

(2) Coordinate with DoD Components to maintain the DoDI 6055.17 installation all-hazards threat assessment (AHTA) to support all MA programs and activities in determining specific hazards and threats, ranging from natural events, human-caused events (accidental and intentional), or technologically caused events.

b. Synchronizes EM, chemical, biological, radiological, and nuclear (CBRN) survivability, operational energy, energy resilience, munitions operations risk management, control systems, and fire protection and prevention with MA by ensuring each program or activity:

(1) Develops program standards and requirements to support the MAAP and provides these to the CJCS, and works with the CJCS to develop MAAP benchmarks for each.

(2) Reviews related risks discovered by the MAAP and updates policy and guidance to address systemic issues, as required.

(3) Provides MA system of record requirements to the Director, DTRA.

(4) Provides representation at the MA SSG for related issues.

(5) Updates related security or protection standards for DCI and MA priorities, as applicable.

(6) Incorporates the principles of the MA Construct in guiding policies.

c. Establishes policy for maintaining infrastructure media files of installation utilities including electrical, water, fuels, natural gas, and communication on the MA system of record.

d. Designates an OPR to identify, analyze, and address strategic risk issues related to DoD-owned and commercial and utility infrastructure, including the associated platform information technology, industrial control systems, and supervisory control and data acquisition systems that support DCI and strategic mission execution.

2.7. DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY. Under the authority, direction, and control of the USD(A&S), and in addition to the responsibilities in Paragraphs 2.19. and 2.20., the Director, Defense Contract Management Agency:

a. Designates an MA OPR to serve as a center of excellence for DIB supply chain network and related analysis to identify, analyze, and address strategic DIB issues that support mission execution and to assist other DoD Components' efforts with DIB-related analysis.

b. Provides necessary subject matter experts (SMEs) to meet MAA team requirements, as required.

(1) Develops program standards and requirements for supporting materiel and services to support the MAAP and provides these to the CJCS.

(2) Works with the CJCS to develop MAAP benchmarks for supporting materiel and services.

c. Enforces contractual requirements relating to cybersecurity.

2.8. DIRECTOR, DTRA. Under the authority, direction, and control of the USD(A&S), and in addition to the responsibilities in Paragraphs 2.19. and 2.20., the Director, DTRA:

a. Establishes a center of excellence for MAAs under the MAAP that provides necessary SMEs, or coordinates to receive necessary SME augmentation from other DoD Components, to meet CJCS prescribed MAA and mobile training requirements.

b. Chairs a working group to:

(1) Document MAA best practices.

(2) Provide DTRA's MAA methodology training to other DoD Components.

(3) Help develop DoD MAA benchmarks.

c. Conducts strategic vulnerability analysis to identify trends impacting defense critical capabilities and missions.

d. Conducts MAAs on DCAs and MACB-prioritized DCI, in collaboration with the responsible Service or Defense Agency and, for non-DoD-owned DCAs and DCI, the asset owner, and provides identified strategic risks to the DASD(DC&MA) and CJCS. These MAAs will include adversarial approach analysis, vulnerability analysis, and enhanced cyber analysis.

(1) Adversarial approach analysis will evaluate the asset or site and supporting infrastructure and identify potential attack vectors based on potential opportunities and known adversary intent and capabilities.

(2) Vulnerability analysis will identify vulnerabilities related to the critical capability, asset, and supporting infrastructure based on the appropriate MA-related programs' and activities' benchmarks and potential attack vectors identified in the adversarial approach assessment. To complete the MAA, DTRA will correlate these vulnerabilities with associated threats and hazards to determine risks to mission execution.

(3) Enhanced cyber analysis will implement cyber assessment requirements prescribed by the DoD CIO for the DoD-owned asset to identify vulnerabilities and determine risk to mission execution. Enhanced cyber analysis will include:

(a) Review of MRT-C submissions on any DCI to be assessed. DTRA will review the MRT-C submissions stored in the Mission Assurance Decision Support System and request any additional information or updates from the asset owner.

(b) On-network information and traffic collection. Coordinate with appropriate Components to grant enterprise authorization for connections.

(c) Collection of an inventory, or verification of an asset owner's inventory, of all hardware, software, and related control systems the asset or capability depends upon. The updated cyber inventory will be provided to the asset owner, the National Security Agency, and

United States Cyber Command (USCYBERCOM) via Joint Force Headquarters-DoD Information Network for further trend analysis and potential vulnerability remediation.

(d) Collection and review of any Mission-Based Cyber Risk Assessments conducted on the TCAs and DCAs in accordance with DoDI 5000.89.

(4) MAA teams will coordinate with the Department of Homeland Security, Federal Bureau of Investigation, and other appropriate LE and counterintelligence agencies to evaluate the specific threats to the critical capability, asset, installation, or supporting commercial infrastructure.

(5) MAA teams will correlate identified vulnerabilities with hazards specific to asset locations and threats identified by intelligence and LE agencies to assess and document the risk to mission execution.

(6) MAA teams will provide the DASD(DC&MA) and CJCS with findings of strategic risk to the mission, capability, force, and assets within 15 working days of completion on the on-site assessment.

(7) DTRA will participate in initial MA SSGs for reviewed MAAs to address questions on the MAA process, significant findings of the MAA, and associated systemic trends across multiple MAAs, as applicable.

e. Establishes a center of excellence to lead the development and management of the MA system of record by consolidating DoD Component requirements and integrating data from MA-related programs and efforts to provide decision-makers with the necessary information for risk management decisions. This will include procedures to reference:

(1) The Defense Intelligence Agency (DIA) global baseline threat assessment data.

(2) The DIA DCI threat assessments, produced for specific sites and DCI.

(3) The center of excellence for supporting infrastructure analysis.

(4) Department of the Air Force advanced analytical assessments.

(5) Defense Contract Management Agency DIB-specific analysis, as applicable.

(6) Threat and hazard supplements for CCMDs with geographic areas of responsibility (AORs) when developing the AHTA, which can include TOP SECRET or higher level data.

2.9. DIRECTOR, DEFENSE LOGISTICS AGENCY. Under the authority, direction, and control of the USD(A&S), and in addition to the responsibilities in Paragraphs 2.19. and 2.20., the Director, Defense Logistics Agency designates an MA OPR to identify, analyze, and address strategic logistic issues that support mission execution and assist other DoD Components' efforts with logistic-related analysis.

2.10. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)). In addition to the responsibilities in Paragraph 2.19., the USD(I&S):

a. Integrates and synchronizes and the Defense Intelligence Enterprise and programs listed under the Defense Security Enterprise (DSE) and LE with MA to ensure DoD Components and subordinate commands account for critical capabilities, and DCI, in these programs' activities.

(1) Establishes intelligence collection and counterintelligence policy and priorities to support MA activities.

(2) Develops program standards and requirements to support the MAAP and provides these to the CJCS, and works with the CJCS to develop MAAP benchmarks for each.

(3) Reviews related risks discovered by the MAAP and updates policy and guidance to address systemic issues, as required.

(4) Provides related MA system of record requirements to the Director, DTRA.

(5) Provides representation at MA SSG for related issues.

(6) Updates security or protection standards for DCI and MA priorities, as applicable.

(7) Incorporates the principles of the MA Construct in guiding policies.

(8) Programs under the DSE include:

(a) Information Security in accordance with DoDI 5200.01.

(b) Physical Security in accordance with DoDI 5200.08.

(c) Industrial Security in accordance with DoDI 5220.22.

(d) Personnel Security in accordance with DoDI 5200.02.

(e) Insider Threat Program in accordance with DoDD 5205.16.

(f) Cybersecurity in accordance with DoDI 8500.01.

(g) Operational Security in accordance with DoDD 5205.02E.

b. Designates an MA OPR to identify, analyze, and address strategic intelligence issues that support mission execution and assist other DoD Components' efforts with intelligence-related analysis.

c. Plans, integrates, coordinates, directs, synchronizes, and manages intelligence support to MA. Coordinates with other appropriate Federal agencies, such as the Department of Homeland Security and the Federal Bureau of Investigation, to obtain threat information that would affect systems and assets related to MA.

(1) Coordinates MA-related activities with the Director of National Intelligence, as applicable.

(2) Designates to the CJCS and the USD(P) those specific intelligence assets outside the scope of MA and not to be included on the MA system of record.

d. Coordinates access for MAA teams to assess intelligence assets at locations nominated by USD(I&S) or MACB-prioritized DCI.

2.11. DIRECTOR, DIA. Under the authority, direction, and control of the USD(I&S), and in addition to the responsibilities in Paragraphs 2.19. and 2.20., the Director, DIA:

a. Produces, triennially or more frequently if required, a secret-level all-source MA baseline threat assessment addressing the following priority intelligence requirements:

(1) Foreign intelligence threats.

(2) Foreign intelligence or counterintelligence insider threats.

(3) Foreign CBRN threats.

(4) Foreign emerging technologies threats.

(5) Foreign cyber threats.

(6) Foreign special operations forces threats.

(7) International terrorism threats.

(8) Foreign threats to space.

(9) Hazards posed by epidemics and pandemics related to MA.

(10) Foreign conventional military and kinetic threat capabilities.

b. Posts assessments to the MA system of record in a format that can be automatically applied to AHTAs along with notifications of and directions to any additional applicable information maintained on higher classification systems.

c. Makes intelligence-based indications and warning information related to MA available to DoD Components and the intelligence community, and communicates to DoD Components credible and actionable data concerning changes in threats.

d. Produces triennially a DCI threat assessment for each DCA and other MACB-prioritized DCI.

e. Provides relevant intelligence, counterintelligence, and threat data on DCAs and other MACB-prioritized DCI to the MA SSG and MA ESG to facilitate risk management recommendation development as resources permit.

f. Approves the provision of intelligence and threat data on DCAs and other MACB-prioritized DCI to the MA SSG and MA ESG to facilitate risk management recommendation development.

2.12. UNDER SECRETARY OF DEFENSE COMPTROLLER/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO). In addition to the responsibilities in Paragraph 2.19., the USD(C)/CFO:

a. Provides guidance and actions, as needed, on funding issues to meet MA requirements and priorities.

b. Reviews budget requirements provided by the MACB and ensures alignment with National Defense Strategy and DoD budget requirements.

2.13. DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE. Under the authority, direction, and control of the USD(C)/CFO, and in addition to the responsibilities in Paragraphs 2.19. and 2.20., the Director, Defense Finance and Accounting Service, designates an MA OPR to identify, analyze, and address strategic finance issues that support mission execution and assist other DoD Components' efforts with finance-related analysis.

2.14. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). In addition to the responsibilities in Paragraph 2.19., the USD(P&R):

a. Designates an MA OPR to identify, analyze, and address strategic manpower or personnel issues that support mission execution and assist other DoD Components' efforts with manpower or personnel-related analysis.

b. Integrates readiness reporting with MA by:

(1) Establishing policy, in coordination with the USD(P), for maintaining DCI-related readiness tracking.

(2) Integrating readiness reporting with the MA system of record.

c. Synchronizes readiness activities with MA by ensuring each effort:

(1) Develops program standards and requirements to support the MAAP and provides these to the CJCS, while working with the CJCS to develop MAAP benchmarks.

(2) Reviews related risks discovered by the MAAP and updates policy and guidance to address systemic issues, as required.

(3) Provides related MA system of record requirements to the Director, DTRA.

(4) Provides representation at the MA SSG for related issues.

(5) Updates security or protection standards for DCI and MA priorities, as applicable.

(6) Incorporates the principles of the MA Construct in guiding policies.

2.15. ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS. Under the authority, direction, and control of the USD(P&R), the Assistant Secretary of Defense for Health Affairs:

a. Designates an MA OPR to provide advice and address strategic Military Health System (MHS) and Force Health Protection (FHP) issues that support mission execution.

b. Integrates MHS and FHP reporting with MA by:

(1) Establishing policy for maintaining MHS DCI-related tracking.

(2) Providing oversight for MHS and FHP reporting integration with the MA system of record.

c. Provides representation at the MACB for related issues.

d. Incorporates the principles of the MA Construct in guiding policies.

2.16. DIRECTOR, DEFENSE HEALTH AGENCY. Under the authority, direction, and control of the Assistant Secretary of Defense for Health Affairs, and in addition to the responsibilities in Paragraphs 2.19. and 2.20., the Director, Defense Health Agency:

a. Designates an MA OPR to identify, analyze, and address strategic health issues that support mission execution and assist other DoD Components' efforts with health-related analysis.

b. Develops MHS and FHP program standards and requirements to support the MAAP and provides these to the CJCS.

(1) Works with the CJCS to develop MAAP benchmarks for each effort.

(2) Coordinates support for MAAs requiring DoD health-related SMEs for Force Health Protection Benchmark assessments.

c. Reviews MHS and FHP-related risks discovered by the MAAP to:

(1) Recommend updates to policy and guidance to address systemic issues, as required.

(2) Assist other DoD Components with MHS and FHP risk management efforts.

d. Provides MHS and FHP-related MA system of record requirements to the Director, DTRA.

e. Updates FHP standards for DCI and MA priorities, as applicable.

2.17. DOD CIO. In addition to the responsibilities in Paragraph 2.19., the DoD CIO:

a. Provides guidance, oversight, and advocacy for the development and management of the MA system of record to ensure decision-makers have the necessary information for risk management decisions.

b. Integrates cybersecurity with MA, in conjunction with the ASD(HD&HA) and CDRUSCYBERCOM, by overseeing implementation of cybersecurity requirements for DoD-owned portions of DCI.

c. Synchronizes cybersecurity implementation with MA, in conjunction with CDRUSCYBERCOM, by ensuring this effort:

(1) Develops program standards and requirements to support the MAAP and provides these to the CJCS, while working with the CJCS to develop MAAP benchmarks for cybersecurity.

(2) Reviews related risks discovered by the MAAP and updates policy and guidance to address systemic issues, as required.

(3) Establishes related MA system of record requirements.

(4) Provides representation at the MA SSG for related issues.

(5) Updates cybersecurity or protection standards for DCI and MA priorities, as applicable.

(6) Incorporates the principles of the MA Construct in guiding policies.

d. Establishes and maintains authority-to-connect (ATC) processes, overseen by the DoD Information Security Risk Management Committee, to facilitate assessments.

2.18. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY. Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in Paragraphs 2.19. and 2.20., the Director, Defense Information Systems Agency:

a. Designates an MA OPR to identify and assess cyber and communication-related strategic risk issues on an end-to-end basis. This will incorporate both DoD-owned and commercial leased voice data communication, and storage capabilities that support mission execution, and assist other DoD Components' efforts with cyber and communication-related analysis.

b. Supports MAAs by providing long-haul analysis of mission information transmission requirements and identifies vulnerabilities in these pathways to the MAA team no less than 60 calendar days before on-site assessment.

c. Designates an MA OPR to serve as a center of excellence for DISN network and related analysis to identify, analyze, and address strategic DISN issues that support mission execution and to assist other DoD Components' efforts with DISN-related analysis.

d. Provides necessary subject matter experts (SMEs) to meet MAA team requirements, as required.

(1) Develops program standards and requirements for supporting DISN services to support the MAAP and provides these to the CJCS.

(2) Works with the CJCS to develop MAAP benchmarks for DISN services.

2.19. DOD COMPONENT HEADS, UNDER SECRETARIES OF DEFENSE, AND THE DOD CIO. The DoD Component heads, Under Secretaries of Defense, and the DoD CIO:

a. Implement the MA Construct described in Section 3 of this issuance.

b. In accordance with Section 3 of this issuance, perform mission owner requirements for the respective component's assigned strategic missions, as applicable:

(1) In the Identification Process by:

(a) Decomposing assigned strategic missions based upon specified or implied tasks, or based upon the universal joint task list (UJTL), to define and provide mission-essential capabilities, standards, and conditions to appropriate DoD Components for task critical asset (TCA) identification.

(b) Proposing related Tier 1 and Tier 2 TCAs.

(c) Validating related recommendations for Tier 1 and Tier 2 TCAs.

(d) Submitting a mission impact statement to the MA system of record for each related, validated Tier 1 and Tier 2 TCA and other MACB-prioritized DCI required for defense critical mission mapping.

(e) Submitting available baseline elements of information (BEIs) to the MA system of record for related, validated non-DoD owned TCAs.

(f) Monitoring the accuracy of data in the MA system of record for related, validated Tier 1 and Tier 2 TCAs and associated BEIs. Collaborating with TCA owners to ensure data accuracy and forwarding issues of contention on data accuracy to the CJCS for arbitration.

(g) Recommending to the CJCS Tier 1 and Tier 2 TCAs for DCA consideration.

(2) In the Assessment Process by:

(a) Nominating mission-essential capabilities, sites, or installations to the CJCS for an MAA, and developing assessment focus statements for MAAs that support the Component's missions. The nominations must also include appropriate OPR(s) for coordinating and granting ATC, in accordance with governing policies, to facilitate on-network cybersecurity assessments during the MAAs.

(b) Providing oversight of MAAs for related, validated Tier 1 and Tier 2 TCAs, as applicable.

(c) Reviewing MAA results related to assigned strategic missions.

(d) Completing a risk assessment for each assigned strategic mission and submitting inputs to the Chairman's Risk Assessment, as appropriate.

(3) In the Risk Management Process by:

(a) Providing recommended remediation priorities to appropriate TCA owners.

(b) Developing and exercising MMPs for the component's mission-essential capabilities. Include completed MMPs, signed by the component head or deputy, in campaign plans, OPLANs, CONPLANs, and COOP plans, as appropriate.

(c) Working with appropriate asset owners to achieve acceptable risk for assigned strategic missions. Asset owners will ensure MAA-compiled cyber inventories are maintained, updated, and reflected in MRT-C submissions to the Mission Assurance Decision Support System.

(d) Supporting established working groups to develop RMPs for mission-essential capabilities supported by DCAs and MACB-prioritized DCI.

(4) In the Monitoring Process by:

(a) Monitoring the operational status of the component's validated Tier 1 and 2 TCAs.

1. Providing to the CJCS and appropriate CCMD with geographic areas of responsibility the mission impact and any Component response for operational status changes.

2. Integrating and leveraging existing DoD operational reporting and situational reporting processes.

(b) Maintaining awareness of risk management action execution. Addressing concerns with appropriate DoD Components and arbitrating unresolved concerns through the MACB.

(c) Monitoring potential threats and hazards to DCAs and Tier 1 and Tier 2 TCAs, and providing threat or hazard advisories to other DoD Components, as appropriate.

c. Establish an MA forum structure at all appropriate organizational levels to support the identification, assessment, risk management, and monitoring of strategic mission-related risks.

d. Ensure the component's MA-related program and activity leads coordinate and synchronize efforts with the component's designated MA OPR.

e. Adapt the MA Construct to OPLANs, CONPLANs, and campaign plans beyond normal day-to-day (Phase 0 Shape) operations, as applicable, to address related Phase 1 through 5 activities. Examples include, but are not limited to:

(1) Prescribing under which phases capabilities and assets are critical or when to execute mitigation plans.

(2) Prescribing when security measures will be added or ensuring plans account for facility security and military operation execution while conducting noncombatant evacuation and deployment of forces.

f. Coordinate and collaborate execution of the MA Construct among components, within component headquarters organizations, and at all operational and administrative levels of the component, including, but not limited to, sharing results of appropriate MA processes with supporting entity leads at appropriate levels, such as with local engineering and communications leads, to prioritize and implement risk reduction activities, etc.

2.20. SECRETARIES OF THE MILITARY DEPARTMENTS; COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND; CHIEF, NATIONAL GUARD BUREAU (IN COORDINATION WITH THE NATIONAL GUARD ADJUTANTS GENERAL OF THE STATES); AND DIRECTORS OF DEFENSE AGENCIES AND DOD FIELD ACTIVITIES. In addition to Paragraph 2.19., the Secretaries of the Military Departments; Commander, United States Special Operations Command (USSOCOM); Chief, National Guard Bureau (in coordination with the National Guard Adjutants General of the States); and Directors of Defense Agencies and DoD Field Activities:

a. Integrate MA forum structure at all appropriate levels of command with other similar requirements such as the AT Working Group.

b. In accordance with Section 3 of this issuance, perform capability provider and asset owner activities for those DCI for which the component has fiscal responsibility:

(1) In the Identification Process by:

(a) Evaluating mission owner-submitted Tier 1 and Tier 2 TCAs and providing analysis on any alternative means to meet the mission-essential capability requirements for those assets.

(b) Ensuring subordinate commands complete execution capability analysis to identify task assets (TAs) related to those assigned tactical-level UJTL tasks or Service or Agency mission-essential task lists (METLs) in the Defense Readiness Reporting System (DRRS) and DRRS-Strategic (DRRS-S). Ensure DRRS and DRRS-S data supports and reflects MA activities, as required. DoD Components and subordinate commands without DRRS or DRRS-S requirements do not perform this activity.

(c) Verifying subordinate commanders incorporate TAs, TCAs, and DCAs in appropriate local-level programmatic risk management activities, as applicable.

(d) Linking mission owner's mission-essential capabilities, standards, and conditions to subordinate commands' mission execution capability analysis to identify potential TCAs. For DoD Components and subordinate commands without DRRS reporting requirements, analyze mission owner-essential capabilities, standards, and conditions to identify TAs and potential TCAs. Providing potential TCAs to mission owners for validation.

(e) Submitting identification process-related BEIs for mission owner-validated DCAs and Tier 1 and Tier 2 TCAs and other MACB-prioritized DCI required for defense critical mission mapping within 90 days of validation to the MA system of record.

(f) Maintaining the accuracy of DCI submissions in the MA system of record and forwarding issues of contention to the CJCS for arbitration.

(g) Ensuring subordinate commands, including those acting as tenants, notify their local commander/host when designated as a Tier 1 or Tier 2 TCA or DCA. Tenants will collaborate with hosts to implement the MA Construct, as required.

(h) Identifying and collaborating with the Air Force's center of excellence and other appropriate entities, including, as applicable and as authorized by law, regulation, and policy, Federal, State, or local LE agencies and commercial security companies, in support of designated TCAs within 30 calendar days of designation; ensure notification of any significant changes or trends in the threat posture against any TCA, whether located in or outside the United States, to the Air Force's center of excellence.

(2) In the Assessment Process by:

(a) Ensuring subordinate commands complete a SECRET-level AHTA in accordance with DoDI 6055.17 and Volume 1 of DoDI O-2000.16 annually, and 30 days prior to receiving an MAA. Heads of the Military Departments or Defense Agencies may approve a waiver of up to 6 months for annual AHTA production if the subordinate command must also produce an AHTA to support an MAA during that time period. The AHTA will consider the DIA global baseline assessment, the CCMD with geographic areas of responsibility AOR supplemental assessment, and local conditions. The completed AHTA will be posted to the MA system of record.

(b) Ensuring appropriate subordinate commands perform the annual self-assessment/inspection requirements from MA-related programs and activities and upload results to the MA system of record in accordance with CJCS-published guidance.

(c) Ensuring subordinate commands meet the established minimum periodicity requirements for an MAA. Subordinate commands will support execution of MAAs related to their missions or installation. Mission or asset owners may request assessment periodicity waivers from the CJCS based on recommendations dealing with the time since the last assessment, on-going remediation actions, etc.

(d) Conducting Military Department or Defense Agency-led MAAs of DCI and installations based upon the standards and conditions required for strategic mission execution established in the mission-owner provided assessment focus statements.

(e) Coordinating Military Department or Defense Agency-performed MAAs with the CJCS.

(f) Providing sufficient SMEs to meet Military Department or Defense Agency-led MAA team needs as defined by the CJCS-published supplemental guidance. SME support may be achieved through augmentation from other DoD Components.

(g) Providing sufficient SME support for MAA teams to meet any additional Military Department or Defense Agency requirements, as required.

(h) Ensuring an inventory of all hardware, software, and related control systems the asset(s) and capability being assessed depends upon is reflected in the asset owner's MRT-C submission; providing the MRT-C to the MAA team upon request. This inventory should be completed to at least the device level (e.g., a Siemens programmable logic controller, Real-Time Linux Version X) though when possible to the component level (e.g., board-level, application level) or subcomponent level (e.g., individual chips, software libraries) is preferable. Asset owners will aid MAA assessors, using established cybersecurity risk management governance, to facilitate authorization to connect and ensure a successful enhanced cyber analysis during a MAA.

(i) Maximizing cyber ATC for MAA assessments. Components that store MRT-C submissions in the Mission Assurance Decision Support System are only required to provide any changes to this submission to the MAA team.

(j) Posting results of all MAAs for DCAs, Tier 1 and Tier 2 TCAs, and other MACB-prioritized DCI to the MA system of record within timelines and formats as defined by CJCS supplemental published guidance.

(k) Completing a risk assessment for each DCA and Tier 1 or Tier 2 TCA assessed by an MAA.

(3) In the Risk Management Process by:

(a) Sharing risk reduction intentions and timelines with mission owners, seeking to achieve acceptable risk to mission.

(b) For all DCAs and MACB-prioritized DCI, coordinating with appropriate stakeholders to develop risk response plans (RRPs) within timelines and formats as prescribed by

CJCS-published supplemental guidance; posting completed RRPs, signed by the DoD Component head or deputy, to the MA system of record; and briefing the MACB on risk response development, implementation, and results.

(c) For essential capabilities supported by DCAs and MACB-prioritized DCI, supporting established working groups to develop RMPs.

(d) Managing risks to missions below the component mission-essential function (MEF) or CCMD campaign plan, OPLAN, CONPLAN, and core joint mission-essential task (JMET) level.

(e) Resourcing SecDef or DepSecDef-approved RMP actions.

(4) In the Monitoring Process by:

(a) Reporting on Tier 1 and 2 TCAs and DCAs operational status changes in accordance with CJCS-published guidance on operational and situational reporting.

(b) Reporting on the availability of all related Tier 1 and Tier 2 TCAs and DCAs during exercises, real-world events, or contingencies in accordance with CJCS-published guidance on operational and situational reporting.

(c) Reporting changes to risk reduction actions or timelines for DCAs and MACB-prioritized DCI to the MA SSG co-chairs, and for other TCAs in accordance with CJCS-published supplemental guidance.

c. Develop training and education requirements to meet the joint MA-related training standards.

2.21. SECRETARY OF THE AIR FORCE. In addition to the responsibilities in Paragraphs 2.19. and 2.20., the Secretary of the Air Force establishes a center of excellence ("Air Force center of excellence") for dedicated, predictive, data-driven advanced analytic assessments to support improved, proactive, prioritized, and agile MAA processes. In collaboration with the supporting infrastructure analytics center of excellence, the Secretary of the Air Force will provide the center of excellence's analysis to DTRA, Joint Staff Deputy Director Nuclear, Homeland Defense, and Current Operations (J36), and the Office of the DASD(DC&MA) no less than 90 calendar days before on-site assessment and when significant changes or trends are identified in the threat posture against any TCA or DCA, whether located in or outside the United States. The Air Force center of excellence will acquire relevant data and coordinate sharing, collaboration, and analysis of such data with DoD Components and other appropriate entities, including, as applicable and as authorized by law, regulation, and policy, the intelligence community; Federal, State, and local LE agencies; and other appropriate security organizations, including commercial sector security and partners and allies that support the missions of relevant assets. The Air Force center of excellence will analyze:

a. Adversary awareness of the importance of the asset or site.

b. Adversary targeting of the asset or site.

c. Any location within 25 nautical miles of the site to be assessed where adversaries have shown a demonstrated interest.

2.22. CJCS. In addition to the responsibilities in Paragraph 2.19., the CJCS:

a. Oversees the execution of the MA identification process for CCMD campaign plans, OPLANs, CONPLANs, and core JMETs, as outlined in Section 3 of this issuance, and arbitrates disputes on asset criticality between DoD Components.

b. In coordination with DoD Components, develops, publishes, and annually reviews supplemental MA guidance for implementing and facilitating MA Construct activities across the DoD Components, including, at a minimum, guidance on:

(1) Identification process execution, including BEI submission. The CJCS will include establishment of a governance forum for BEI development and approval.

(2) MAA and MA self-assessment execution.

(3) RMP development and coordination, including RRP and MMP enclosures signed by the component head or deputy, for DCAs and MACB-prioritized DCI.

(4) Monitoring, including the MA system of record; TCA reporting for real-world events, exercises, and contingencies; and risk reduction action execution.

c. Manages, on behalf of the MACB, the identification, assessment, and RMP development for DCAs and MACB-prioritized DCI supporting mission-essential capabilities or defense critical missions, with support from appropriate DoD and OSD Components.

d. Designates a system of record to store DCI data, assessment products and results, and RMPs for the MA community. The CJCS establishes and ensures inputs contain minimum BEI requirements, and reviews designated Tier 1 TCAs to support CJCS Manual 3105.01 implementation and data validity.

e. Provides DCA nominations to the ASD(HD&HA), in coordination with the DoD Components, including the OSD Components, along with the opinions of applicable mission and asset owners. In December of each year, validates or recommends DCA list changes to the ASD(HD&HA).

f. Ensures the timely production and posting to the MA system of record of the CCMD with geographic areas of responsibility's AOR hazard assessment and CCMD with geographic areas of responsibility AOR supplement to the DIA global baseline threat assessment.

g. Implements and oversees the MAAP in accordance with CJCS policy on MAAs (e.g., Joint Staff MAA Concept of Operations, April 2016).

(1) Provides guidance for execution of the MAAP.

(2) Follows established periodicity criteria to designate assessment timelines.

(a) Ensures DoD Components meet periodicity requirements.

(b) Adjudicates mission owner assessment periodicity windows with each asset owner. Minimizes overlapping assessments or unnecessary duplication of efforts.

(c) Reviews and grants waivers to periodicity requirements submitted by the DoD Components.

(3) Standardizes MAA activities across DoD, including issuing integrated MA benchmarks and standards for use by all teams, at a minimum, in coordination with other DoD Component heads.

(4) Provides guidance for collecting self-assessment and self-inspection results from MA-related programs and activities.

(5) Develops and manages execution of an annual department-wide MAAP schedule. Coordinates the schedule with DTRA, Military Departments, and appropriate Defense Agencies to synchronize efforts and reduce the annual burden of multiple assessment team visits to the same location.

(6) Ensures a DTRA MAA is conducted on all DCAs and MACB-prioritized DCI.

(a) DTRA MAAs have priority over Military Department or Defense Agency MAAs when assessing subordinate commands/installations housing DCAs or MACB-prioritized DCI.

(b) To reduce duplication of effort, Military Department or Defense Agency MAA teams may accompany or supplement a MAA to assess other TCAs assessed at the subordinate command/installation not covered by the MAA.

(7) Ensures all MAA results are posted to the MA system of record.

(8) Briefs the MACB on MAAP risk findings for DCAs and MACB-prioritized DCI supporting defense critical missions.

h. In support of the ASD(HD&HA), provides recommendations on joint MA-related training and education programs for the Department.

i. Designates the Director, Joint Staff as the MA ESG co-chair and the Vice Director, Joint Staff as the MA SSG co-chair.

2.23. COMBATANT COMMANDERS. In addition to the responsibilities in Paragraph 2.19., the Combatant Commanders:

a. Collect and disseminate MA-related threat assessments and warnings, as appropriate, to subordinate elements, the Air Force center of excellence, and other DoD Components.

b. Include appropriately developed MMPs in the command's applicable campaign plans, OPLANs, and CONPLANs.

c. Align MA risk management efforts with the CCMD's integrated priority list and issue paper processes.

d. Execute established MMPs, when required. Integrate evaluation or execution of MMPs into exercises, as applicable.

e. Implement MA at the operational level to identify, assess, manage risk, and monitor essential capabilities supporting CCMD, CCMD with geographic areas of responsibility, sub-unified command, component, and supporting agency mission-essential tasks (METs).

f. Establish, synchronize, and monitor MA METs identified by MA-related protection programs via DRRS. Synchronize effort with CCMDs with geographic areas of responsibility, sub-unified commands, components, and supporting agencies to leverage policies, reporting, and information-sharing mechanisms across protection programs.

2.24. COMBATANT COMMANDERS WITH GEOGRAPHIC AREAS OF RESPONSIBILITY. In addition to the responsibilities in Paragraphs 2.19. and 2.23., the Combatant Commanders with geographic areas of responsibility:

a. Produce an AOR-specific supplement to the global baseline threat assessment and an AOR-specific hazard assessment that address natural disaster and severe weather potentials. Post these assessments to the MA system of record.

b. In coordination with asset owners, monitor changes to the operational status of Tier 1 and Tier 2 TCAs within the AOR and provide CCMD with geographic areas of responsibility AOR situational awareness to applicable DoD Components in accordance with CJCS-published operational reporting and situational reporting guidance.

2.25. COMMANDER, UNITED STATES TRANSPORTATION COMMAND. In addition to the responsibilities in Paragraphs 2.19. and 2.23., the Commander, United States Transportation Command, designates an MA OPR to identify and assess transportation-related strategic risk issues that support mission execution, and assist other DoD Components' efforts with transportation-related analysis.

2.26. COMMANDER, UNITED STATES SPACE COMMAND (USSPACECOM). In addition to the responsibilities in Paragraphs 2.19. and 2.23., the Commander, USSPACECOM, designates an MA OPR to identify and assess space-related strategic risk issues that support mission execution, and assist other DoD Components' efforts with space-related analysis.

2.27. CDRUSCYBERCOM. In addition to the responsibilities in Paragraphs 2.19. and 2.23., the CDRUSCYBERCOM:

a. Synchronizes, in coordination with USD(P), the MRT-C effort with MA to provide to mission owners' TAs and potential TCAs identified by mission-relevant terrain analysis.

b. Coordinates and leverages capabilities of USCYBERCOM's assessments with MAAs. Shares assessment results within the MA system-of-record.

c. Aligns cybersecurity and cyber defense capabilities on the basis of mission risk and ASD(HD&HA) guidance. Ensures DCI receive appropriate cyber protection.

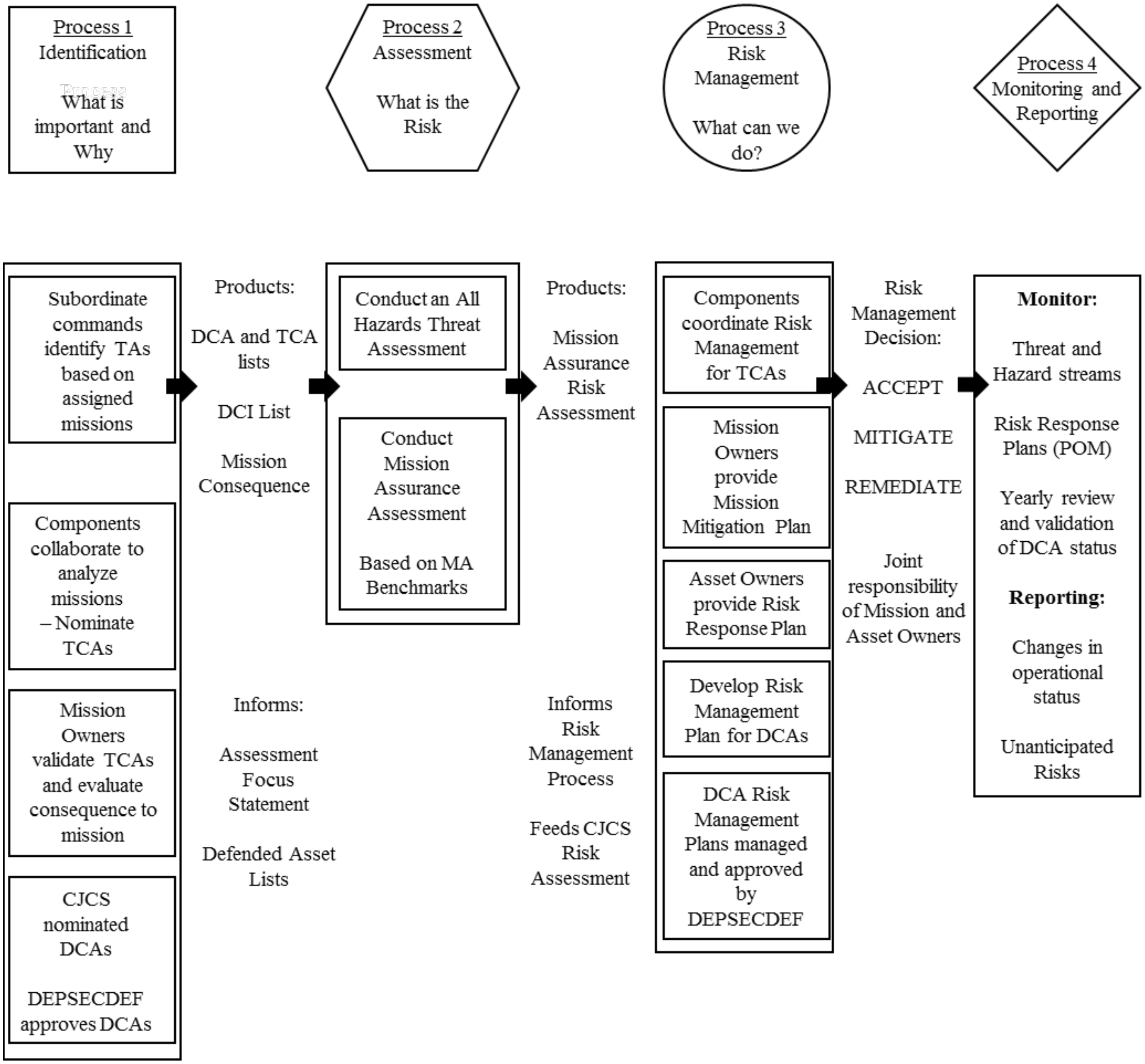
d. Provides information on cyber threat changes impacting DCAs, Tier 1 TCAs, and Tier 2 TCAs, as appropriate, to mission and asset owners.

e. Through the Mission Assurance Decision Support System, evaluates impacts on and risk to mission from emerging cyber vulnerabilities and provide reports of the risks related to DCAs and MACB-prioritized DCI to the DASD(DC&MA), Joint Staff, CCMDs, Military Departments, and other appropriate DoD Components.

SECTION 3: MA CONSTRUCT

3.1. MA CONSTRUCT. MA seeks to prioritize DoD efforts and resources toward addressing the most critical strategic mission execution concerns. The MA Construct's four processes are identification, assessment, risk management, and monitoring. Their relationship to one another and products is illustrated in Figure 1.

Figure 1: Mission Assurance Construct


Process 1
Identification
What is important and Why
Process 2
Assessment
What is the Risk
Process 3
Risk Management
What can we do?
Process 4
Monitoring and Reporting
Subordinate commands identify TAs based on assigned missions
Components collaborate to analyze missions – Nominate TCAs
Mission Owners validate TCAs and evaluate consequence to mission
CJCS nominated DCAs
DEPSECDEF approves DCAs
Products:
DCA and TCA lists
DCI List
Mission Consequence
Informs:
Assessment Focus Statement
Defended Asset Lists
Conduct an All Hazards Threat Assessment
Conduct Mission Assurance Assessment
Based on MA Benchmarks
Products:
Mission Assurance Risk Assessment
Informs Risk Management Process
Feeds CJCS Risk Assessment
Components coordinate Risk Management for TCAs
Mission Owners provide Mission Mitigation Plan
Asset Owners provide Risk Response Plan
Develop Risk Management Plan for DCAs
DCA Risk Management Plans managed and approved by DEPSECDEF
Risk Management Decision:
ACCEPT
MITIGATE
REMEDIATE
Joint responsibility of Mission and Asset Owners
Monitor:
Threat and Hazard streams
Risk Response Plans (POM)
Yearly review and validation of DCA status
Reporting:
Changes in operational status
Unanticipated Risks

3.2. INFORMATION SHARING.

a. Need to Share. Sharing information through coordination and collaboration is vital to the success of the MA Construct. Information has strategic value to DoD. It must be safeguarded, appropriately secured, and shared with authorized DoD personnel and mission partners throughout the information's lifecycle. DoD Components performing MA activities will share information, DoD policy, and mission requirements, as allowed by law, with internal component MA program lead OPRs; other DoD Components and DoD entities; interagency partners; State, local, or tribal officials; foreign governments; and private industry representatives, as necessary to implement the MA Construct.

(1) MA Construct implementers also will refer to and follow appropriate security classification and information-sharing policy of the other MA-related programs and efforts before sharing MA information.

(2) Nothing in this issuance prevents DoD Components from sharing, consistent with applicable law and policy, with interagency partners having a need to know and appropriate security clearance MA data and information developed pursuant to their established OCA authorities and not otherwise covered by Paragraph 3.2.c.

(3) Nothing in this issuance supersedes or in any way changes other OCAs' classification decisions. Prior to sharing MA information, the holders of the information must ensure they are following all appropriate OCA guidance related to that information.

b. Access to DoD Data and Databases Containing Assets Identified as DCI.

(1) DoD Components may grant access to their DCI data and their databases for DoD personnel who meet appropriate security requirements for access to this information.

(2) DoD Components may grant limited access to their DCI data and their databases to non-DoD individuals or organizations who meet the appropriate legal and security requirements for accessing the data. These persons are only granted access to limited DCI-related data necessary to that individual or organization to support MA efforts. If the data cannot be provided within such limits, then the DoD Component may only share printed copies of those portions of the database necessary for duty performance.

c. DCI Line of Effort Information.

(1) The ASD(HD&HA) will issue a security classification guide for the DCI line of effort to prescribe the classification of information associated with the terms DCA, TCA, and DCI.

(2) The ASD(HD&HA) is the approval authority for access to the DCA and TCA lists, including subsets, and will issue supplemental guidance on DCI information sharing as necessary. In addition to any applicable legal restrictions, the following guidelines for sharing data associated with the terms DCA, TCA, and DCI apply:

(a) DCAs.

1. Information associated with the term DCA may be shared within DoD with any person who has the appropriate DoD clearance and need to know. This includes non-DoD personnel (federal department and agency personnel including LE) and FIVE EYES (FVEY) personnel permanently assigned to a DoD billet. Access to this information for non-DoD personnel will terminate upon their transfer from DoD.

2. Any other sharing of information associated with the term DCA outside of DoD requires ASD(HD&HA) written approval.

3. Disclosure will be documented by the responsible foreign disclosure officer in accordance with DoD foreign disclosure policy and applicable agreements. Access will be controlled and limited to those aspects necessary for non-DoD and FVEY personnel to accomplish their duties. Information released to FVEY personnel under this process will not be re-marked as releasable to FVEY.

(b) TCAs.

1. Information associated with the term TCA will be shared within DoD with any person who has the appropriate clearance and need to know. This includes non-DoD personnel (Federal department or agency personnel including LE) and FVEY personnel who are permanently assigned to a DoD billet. Access to this information for non-DoD personnel will terminate upon their transfer from DoD.

2. DoD Component heads responsible for creating or managing TCA-associated data may grant access to specific BEIs from their component's designated TCAs to any properly cleared U.S. Government or FVEY person not in a DoD billet but with the need to know who is supporting DoD planning or operations. This information will be handled and disclosed in accordance with all applicable laws, DoD policies, and mission requirements.

3. CCMDs may also share data associated with the term TCA for those assets within their AOR to support preparedness, emergency response, or Defense Support of Civil Authorities activities. This sharing will be in accordance with all applicable laws, DoD policies, and mission requirements.

4. Sharing the DoD TCA list as recorded in the MA database of record outside of DoD requires ASD(HD&HA) written approval.

(c) DCI

1. Unclassified information associated with the term DCI is UNCLASSIFIED and will be shared as allowed by law, DoD policy, and mission requirements.

2. Classified information associated with the term DCI will be shared as allowed by law, governing security classification guidance, other applicable DoD policy, and mission requirements.

(3) DoD personnel will be familiar with non-DoD agency classifications such as sensitive secure information, protected critical infrastructure information, and LE sensitive information before release to ensure proper handling of MA information.

(4) U.S. Coast Guard personnel meeting the established security clearance and need-to-know requirements will be granted access to information associated with the terms DCA, TCA, or DCI as if they were DoD personnel, regardless of their status.

(5) Requests to share information associated with the terms DCA and TCA based on the conditions in Paragraphs 3.2.c.(2)(a)2. and 3.2.c.(2)(b)4. will be submitted in writing (email is acceptable), from a General Schedule (GS)-15/O-6 permanently assigned to the component, and signed by the DoD Component head. This request will be sent to the Director, MA, for staffing. Written approval/disapproval will be transmitted from the ASD(HD&HA) to the DoD Component head.

3.3. IDENTIFICATION PROCESS.

a. Method.

(1) MA Identification Process Goal. The goal of the MA identification process is to synchronize the various MA-related programs and activities to identify a list of mission-essential capabilities as well as a tiered list supporting DCI that facilitates the remaining processes in the MA Construct (Figure 2).

(2) MA Construct. DoD Components are assigned the following roles under the MA Construct:

(a) OSD and DoD Components heads will perform the duties of mission owners for their organizational MEFs created pursuant to DoDD 3020.26.

(b) CCMDs will perform the duties of mission owners for assigned campaign plans, OPLANs, CONPLANs, and core JMETs.

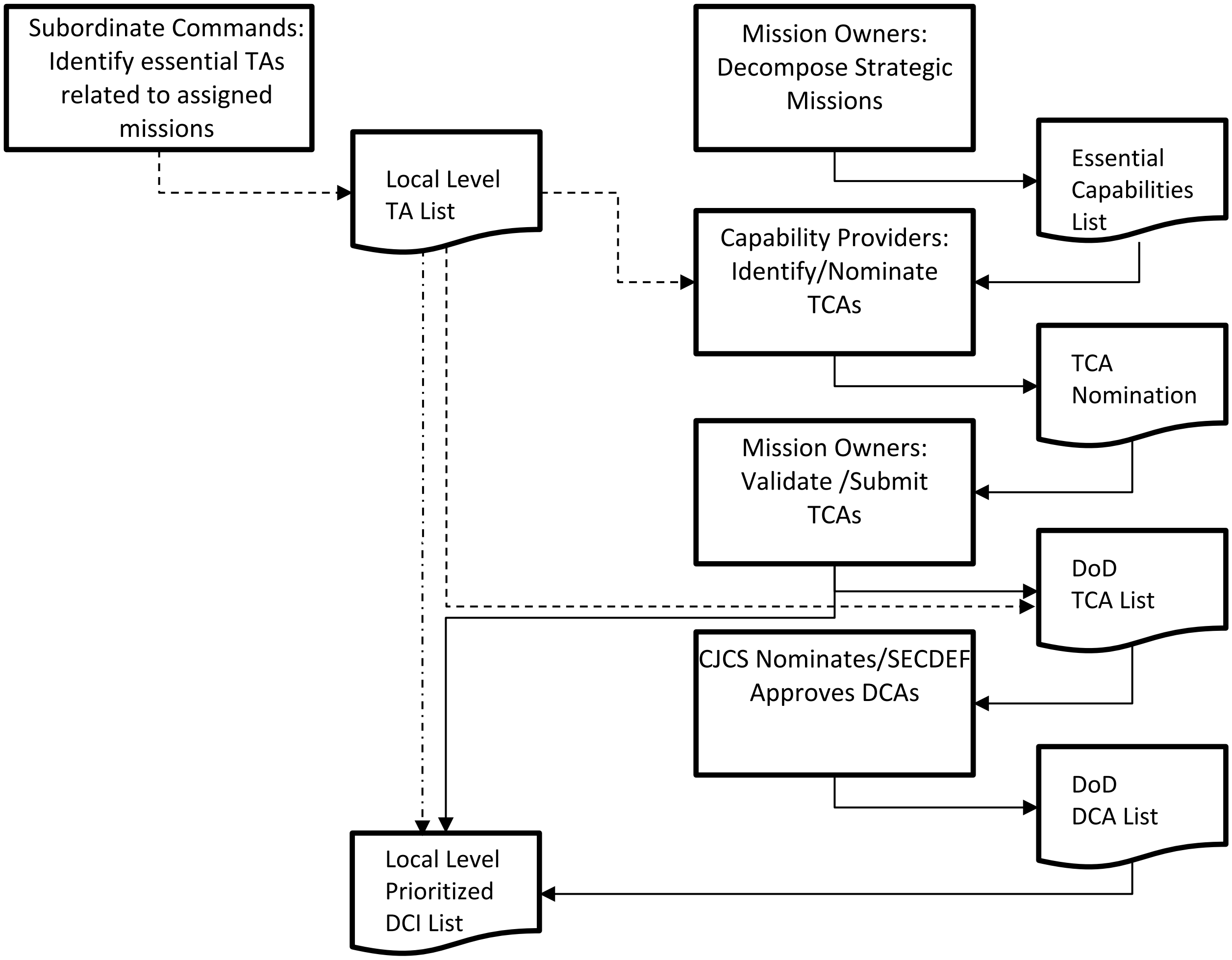
(c) USCYBERCOM, the Military Departments, Service components, Defense Agencies, and DoD Component heads designated responsibility for assisting other components' identification efforts will perform the duties of capability providers.

(d) USSOCOM, the Military Departments, Service components, and Defense Agencies with the resourcing responsibility for a DoD-owned asset will perform the duties of asset owner.

(3) Subordinate Level Capability Execution Analysis. Command structures below the component level, through their established MA forum structure, will identify those TAs required for execution of assigned missions recorded in DRRS and derived from tactical-level UJTL tasks or Service or Agency METLs.

(a) The MA forum will consider all appropriate assets identified as important to mission execution by any of the MA-related programs or activities. The resulting TAs identified in this collaborative process will be reflected in each MA-related program and activity's individual efforts, as applicable.

Figure 2: Identification Process and Results


Subordinate Commands: Identify essential TAs related to assigned missions
Local Level TA List
Mission Owners: Decompose Strategic Missions
Essential Capabilities List
Capability Providers: Identify/Nominate TCAs
TCA Nomination
Mission Owners: Validate /Submit TCAs
DoD TCA List
CJCS Nominates/SECDEF Approves DCAs
DoD DCA List
Local Level Prioritized DCI List

(b) Assets may be people, facilities, or physical objects (e.g., Building 1201, or a network server), information systems or applications (e.g., an emergency message system), or information (e.g., real-time weather data).

(c) Assets may be located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations.

(d) The local MA forum representative for planning or readiness will ensure analysis of all assigned missions.

(e) The readiness lead will ensure DRRS data accurately reflects all assigned missions of the command.

(f) The command will share TA BEI data for MACB-prioritized DCI to support defense critical mission mapping.

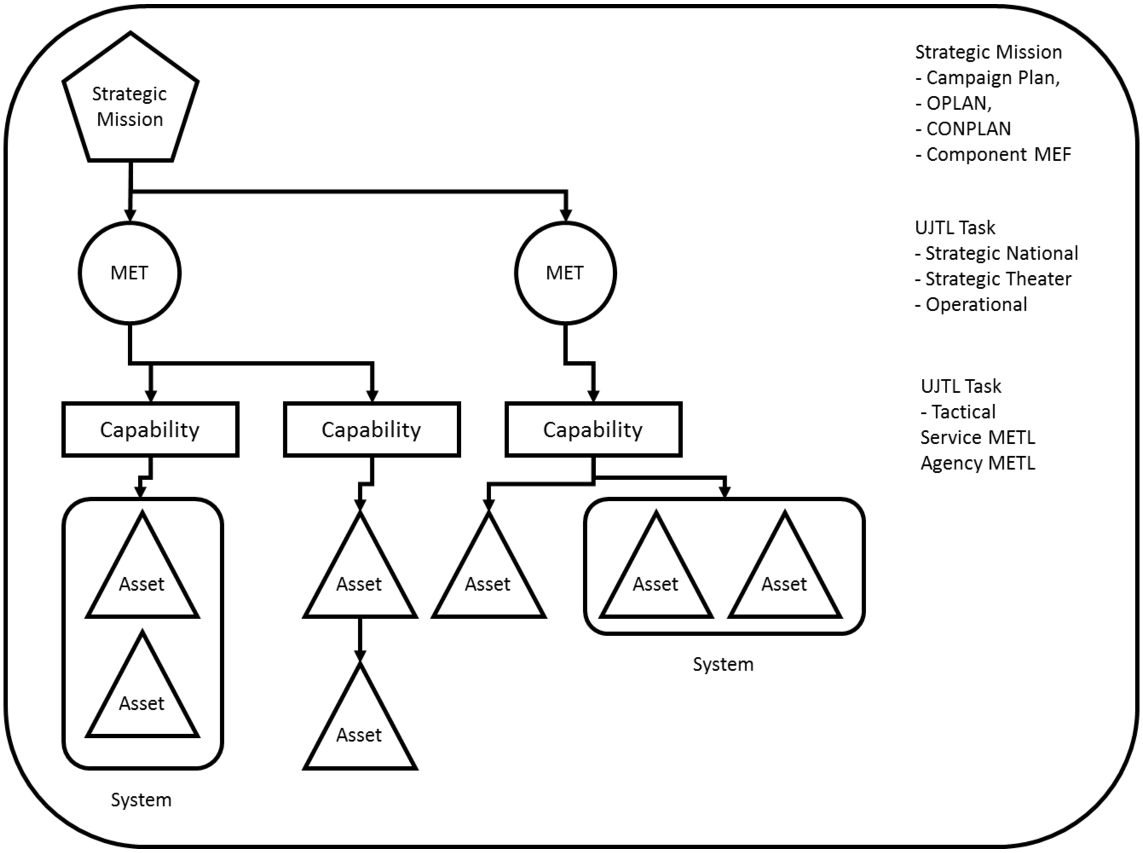
(g) The Military Departments and Defense Agencies will ensure the timely completion and a regular review and update of this analysis by their subordinate command structures.

(4) Component-Level Strategic Mission Analysis. DoD Components decompose their strategic missions through the UJTL structure foundation and then perform collaborative analysis to identify essential capabilities and critical systems and assets.

(a) Step 1 – Conduct Mission Decomposition. Mission owners, supported by appropriate CCMDs with functional areas of responsibility, decompose strategic missions in a three-part process:

1. Part 1: Identifying those strategic national, strategic theater, and operational-level UJTL tasks necessary for execution (Figure 3) in METs.

Figure 3: MA Identification Process Relationships



2. Part 2: From METs into essential capabilities by identifying tactical-level UJTL tasks, or Service or Agency METLs necessary to implement each MET.

3. Part 3: By prescribing the standards (what is needed and how much), the mission-essential capability required to achieve success and the conditions (e.g., where, when, by, or for whom) under which the capability is required.

4. Mission owners record this completed mission decomposition in the MA system of record and provide this analysis to appropriate capability providers.

5. Mission owners will include in this submission any known Tier 1 or Tier 2 TCAs aligned with the appropriate essential capability or UJTL MET.

6. CCMDs with functional areas of responsibility will work with mission owners to provide any additional METs or essential capabilities, along with associated standards and conditions, necessary for CCMD with functional areas of responsibility support to meet mission execution requirements. CCMDs with functional areas of responsibility record this completed mission decomposition in the MA system of record and provide this analysis to appropriate capability providers.

7. CCMDs with functional areas of responsibility will include in this submission any known Tier 1 or Tier 2 TCAs aligned with the appropriate essential capability or UJTL MET.

(b) Step 2 – Identify and Nominate TCAs. Capability providers will link the mission owners' essential capabilities to subordinate commands' capability execution analysis to reveal potential Tier 1 and Tier 2 TCAs, and will submit these results and supporting analysis to mission owners for validation.

1. A TCA is an asset or systems of such extraordinary importance that its incapacitation or destruction would have a serious debilitating effect on an essential capability or MET that will cause severe degradation or failure of the supported strategic mission. TCAs will meet one of the following criteria:

a. No other TA is available to meet the minimum performance standards and conditions of the essential capability resulting in a single point of failure.

b. Multiple similar and functionally related TAs exist, not necessarily co-located in a single geographic location, that must perform together to meet the requirements of the essential capability's minimum performance standards and conditions. The loss of any of these TAs causes the system to fail or significantly degrade (e.g., four locomotives are necessary to meet throughput levels of cargo; the loss of one prevents essential capability accomplishment). This system will be recorded as a single TCA.

c. An alternate TA supporting another essential capability of the same strategic mission is available, but using this alternate TA will cause failure or significant degradation to that other essential capability.

d. An alternative or workaround to the TA exists that could potentially provide the essential capability, but the alternative has not been operationally tested or validated to do so. Until such time as the alternative is certified to meet mission requirements, the original TA will still be considered a TCA.

2. A Tier 1 TCA is an asset whose loss, incapacitation, or disruption will cause a serious debilitating effect on an essential capability or MET and result in strategic mission failure at the OSD Component, Military Department, CCMD, or Defense Agency-level. Mission owners will ensure that the loss of assets validated as Tier 1 TCAs also meet the intent of Joint Risk Analysis Methodology in CJCS Manual 3105.01, "consequence of extreme harm to the execution of a strategic mission." The CJCS will review all Tier 1 TCA ratings.

3. A Tier 2 TCA is an asset whose loss, incapacitation, or disruption will cause a serious debilitating effect on an essential capability or MET and result in strategic mission degradation at the OSD Component, Military Department, CCMD, or Defense Agency-level. Mission owners will ensure that the loss of assets validated as Tier 2 TCAs also meet the intent of Joint Risk Analysis Methodology in CJCS Manual 3105.01, "consequence of major harm to the execution of a strategic mission."

4. Capability providers may also designate Tier 3 TCAs that represent assets from forces not currently assigned to support a strategic mission, but will become Tier 1 or Tier 2 TCAs when linked to a strategic-level mission.

5. Capability providers will:

a. Evaluate the mission owner's and associated CCMD with functional areas of responsibility's submitted Tier 1 and Tier 2 TCAs and provide analysis on any alternatives for each.

b. With support from designated OPRs for specific areas (e.g., logistics, finance), analyze mission owner and CCMD with functional areas of responsibility-submitted essential capabilities, standards, and conditions, and link these to subordinate capability execution analysis to nominate additional potential Tier 1 and Tier 2 TCAs to the mission owner or CCMD with functional areas of responsibilities.

6. CCMDs with functional areas of responsibility will evaluate capability provider-submitted TCA analysis and forward to mission owners the CCMD's recommendations on potential TCAs.

(c) Step 3 – Tier 1 and Tier 2 TCA Validation and Submission. DoD Component heads will validate nominated Tier 1 and Tier 2 TCAs, and components will record results in the MA system of record.

1. The DoD Component heads will validate the effect on strategic mission execution per the criteria in Paragraphs 3.3.a.(4)(b)2.-3. for each nominated TCA and designate the asset as a Tier 1 or Tier 2 asset. Mission owners will notify appropriate asset owners of their DoD Component head's validation results.

2. Mission owners will submit to the MA system of record the mission impact statement for each validated TCA and prescribe the criteria necessary to downgrade or remove TCA designation (e.g., establishing a geographically separate communications pathway, increasing prepositioned materials to support 30 extra days of operations).

3. Mission and asset owners will record BEI data for validated DoD-owned TCAs in the MA system of record.

4. Mission owners will record available BEI data for validated non-DoD owned TCAs in the MA system of record.

5. DoD Components will ensure awareness by command structures below the component level of the designated TCAs over which they have authority. Subordinate command leads for readiness or planning will ensure designated Tier 1 and 2 TCAs are incorporated into the appropriate DRRS reporting process.

6. The component's planning, readiness, and DCI or MA leads will implement this step with the support of all other MA forum leads.

(d) Step 4 –DCA Designation. Based on the Tier 1 and Tier 2 TCAs submitted, and with advice from OSD, the CJCS will nominate DCAs.

1. DCA designation should be reserved for assets whose loss, incapacitation, or disruption could result in mission failure or severe degradation of multiple strategic missions, including the direct defense of the homeland, a vital national capability, a DoD-level MEF, a DoD principal mission-essential function, or a national essential function.

2. The list of DCAs will serve as the primary focus for departmental risk management. The Department's goal is to minimize the number of assets on the DCA list. When efforts to eliminate DCAs are too costly or the timelines to do so are too lengthy, the DoD will prioritize risk management actions to increase the resiliency of those DCAs to ensure their availability to the warfighter.

3. The CJCS will monitor the execution of the Identification Process and provide updates to the MACB highlighting step completion, delays, and results.

4. The CJCS will, in coordination with appropriate mission and asset owners and with the advice of OSD, nominate to the ASD(HD&HA) for SecDef approval a list of DCAs by December of each year based upon Tier 1 and Tier 2 TCA submissions. This will include:

a. Revalidation of existing DCAs.

b. Nominations for adding new DCAs that meet established criteria.

c. Removals of DCA designation for assets no longer meeting DCA criteria.

5. SecDef is the approval authority for the DCA list.

6. The DASD(DC&MA) will notify DoD Components of the approval of the DCA list. The CJCS will post the current approved list to the MA system of record.

7. Asset owners will ensure appropriate subordinate commands are aware of DCAs they have authority over.

(5) MA Forum Leads. MA forum leads will integrate the MA Identification Process results with similar MA-related program and activity efforts such as the AT critical asset matrix, COOP and EM planning, energy resilience, or security program prioritization.

b. Timeline and Result Application.

(1) Each OSD and DoD Component head will complete the identification process every 3 years for each strategic mission and revalidate Tier 1 and 2 TCAs annually.

(2) Because missions and the executing environment are dynamic, mission owners may elect to execute the identification process on only part of a mission, such as one or more METs or essential capabilities, more often, providing the entire mission is analyzed every 3 years.

(3) OSD and DoD Component heads with multiple strategic missions may perform the identification process on a staggered timeline (such as after each OPLAN update) rather than completing all assigned strategic missions concurrently.

(4) The MA Identification Process results provide a tiered focus for assessment, risk management, and monitoring process activities at all levels of command.

(a) The identification process produces the DCI list; the TCA list, a tiered subset of the DCI list; and the DCA list, the highest tiered subset of the DCI list.

(b) At command structures below the component level, the DCI list focuses local MA forum efforts toward protecting and managing the risk to mission-executing assets across all MA-related programs and activities. The TCA and DCA lists provide the commanders at these levels with tiered priorities for risk reduction actions or investments.

(c) At the component level, MA-related programs and activities focus on improving security, protection, and risk management conditions. Commanders address identified mission-related operational and force management risks to strategic missions with a priority on risks related to the TCA and DCA lists.

(d) At the Department level, the DCA list provides a basis for strategic and military-level mission-based risk management across the Department.

3.4. ASSESSMENT PROCESS.

a. Method.

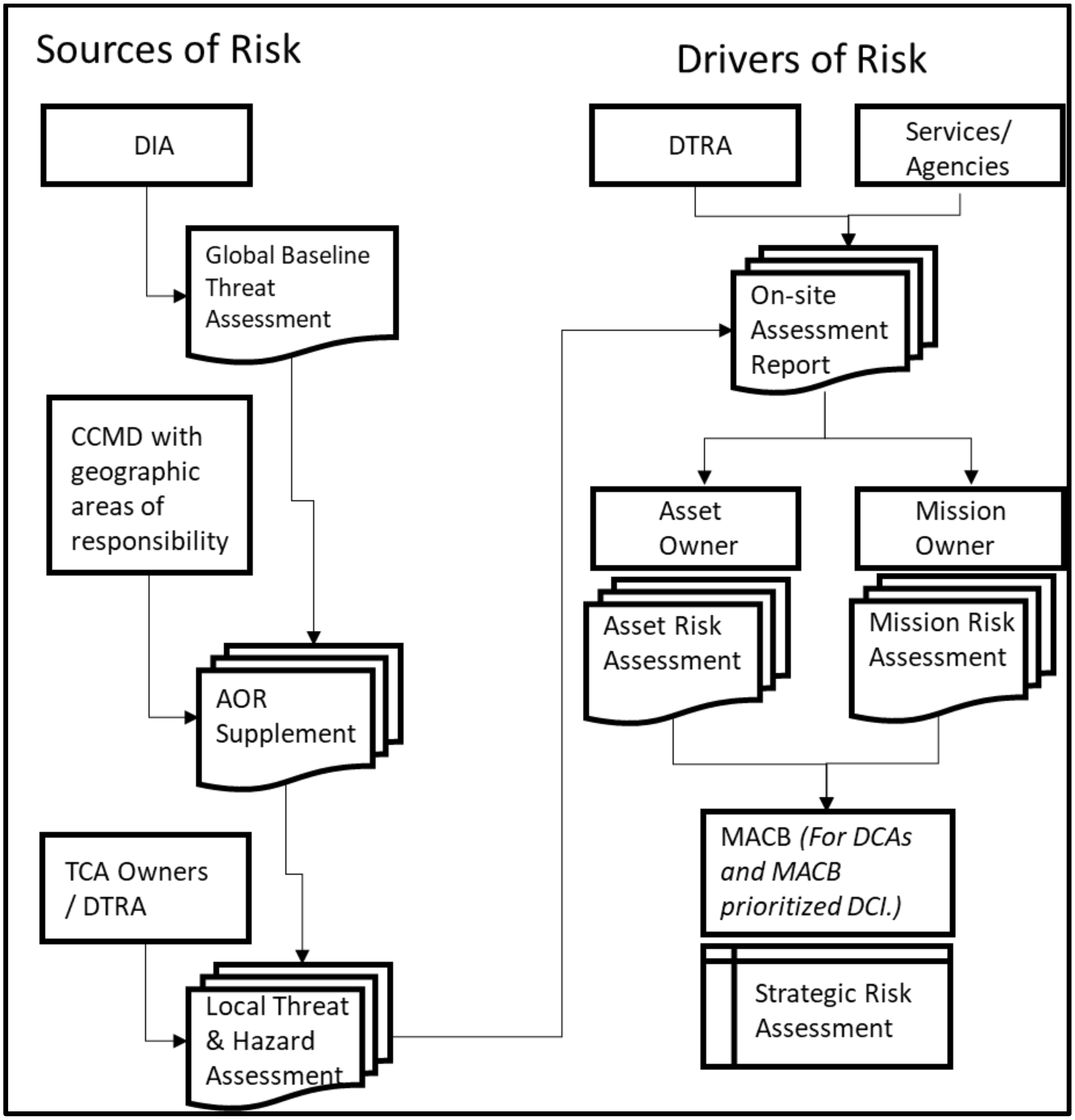
(1) The goal of the MAA process is to integrate the various MA-related programs and activities through an all-inclusive risk management process that determines probabilities and assesses consequences to characterize the risk to assets, systems, and essential capabilities supporting strategic missions (Figure 4). The assessment process is composed of:

(a) Identifying threats and hazards capable of exploiting, denying, deceiving, degrading, disrupting, or destroying the asset or system supporting the essential capability, along with assessing the likelihood of these events occurring. This assessment is conducted based on conditions at the local level through the installation's AHTA for TCAs or by those identified threat and hazard conditions provided by DIA and the Air Force center of excellence used by DTRA to assess strategic risk for DCAs and other MACB-prioritized DCI. AHTA results will be stored in the MA system of record.

(b) Identifying vulnerabilities related to assessed threats and hazards, but with adjustments based on asset, system, or essential capability resilience, accessibility, recognition, and cascading effects. This is accomplished through either the CJCS or Military Department or Defense Agency-led MAAP, and by local-level self-assessments. All MAAP assessments will be conducted in accordance with supplemental CJCS guidance, and results will be stored in the MA system of record.

(c) Evaluating both the threats and hazards and associated vulnerabilities to assess the risk to the asset or system and the mission it supports.

Figure 4: Assessment Process


Sources of Risk
Drivers of Risk
DIA
Global Baseline Threat Assessment
CCMD with geographic areas of responsibility
AOR Supplement
TCA Owners / DTRA
Local Threat & Hazard Assessment
DTRA
Services/ Agencies
On-site Assessment Report
Asset Owner
Mission Owner
Asset Risk Assessment
Mission Risk Assessment
MACB *(For DCAs and MACB prioritized DCI.)*
Strategic Risk Assessment

(2) Activities for sources of risk – threats or hazards that alone or in combination have potential to harm the asset or mission it supports.

(a) Commanders will ensure their MA activity leads integrate the AHTA from DoDI 6055.17, and the Terrorism Threat Assessment from Volume 1 of DoDI O-2000.16, in a combined local-level AHTA to identify and evaluate the sources of risk to assets, systems, and essential capabilities. Commanders will ensure this AHTA is informed by the DIA all-source global baseline threat assessment, the applicable CCMD with geographic areas of responsibility's AOR-specific supplement, and the asset-specific DCI threat assessment and warnings from the Air Force center of excellence database, if either is applicable.

(b) DIA will produce an all-source global baseline threat assessment as outlined in Paragraph 2.11.c. of this issuance and post the results to the MA system of record. As part of this baseline assessment, DIA will provide an evaluation of each near-peer adversary's capabilities and where the capability is likely to be employed on the competition to conflict continuum. DIA will also produce on a triennial basis a DCI threat assessment for each DCA and other MACB-prioritized DCI associated with defense critical missions.

(c) CCMDs with geographic areas of responsibility will produce a global baseline threat assessment supplement for their AOR every 3 years, at a minimum, that includes:

1. Specific deviations from the global baseline threat assessment defined by country or area, and post to the MA system of record.

2. A specific natural disaster and severe weather hazards assessment by country or area, and post to the MA system of record.

(d) The Air Force center of excellence will perform a database query for all assessments of DCAs and other MACB-prioritized DCI. In collaboration with the infrastructure analytics center of excellence, the Air Force center of excellence's analysis will be provided to DTRA, Joint Staff J36, and the Office of the DASD(DC&MA) no less than 90 calendar days before on-site assessment and when significant changes or trends are identified in the threat posture against any TCA or DCA, whether located in or outside the United States.

(e) Appropriate Military Department and Defense Agency commands will, on an annual basis, reference the DIA, CCMD with geographic areas of responsibility, and the Department of the Air Force products to develop or update an AHTA for use across all MA-related programs and activities at the command's level. DTRA will review the local AHTA and supplemental intelligence products to produce updated threats and hazards for assessments of DCAs and other MACB-prioritized DCI and share this assessment with the assessed commands.

1. When AHTA results deviate from threat or hazard levels in the applicable CCMD with geographic areas of responsibility baseline supplement, commanders should document reasons for this deviation.

2. The AHTA will also describe any other local conditions that adjust the assessed level of threat or hazard.

3. For assessing the level of threat from near-peer adversaries, MAAs will follow the following planning assumptions:

a. Intelligence showing one or more near-peer adversaries are actively targeting the critical capability, installation, asset, or its supporting infrastructure will be rated as **high** threat.

b. Intelligence showing one or more near-peer adversaries are aware of the asset's importance or whose doctrine or history show attacks against this type of critical capability, asset, or its supporting infrastructure will be rated as a **significant** threat.

c. Threats to assets that do not meet either of the criteria for significant or high threat will be rated according to the level of threat assigned by DIA.

(3) Assessing vulnerabilities – existing conditions that, if exploited by a known threat or hazard, place mission execution at risk.

(a) The CJCS will implement and oversee an MAAP focusing primarily on observations of conditions and vulnerabilities that can be exploited by the AHTA-identified threats and hazards to degrade mission execution success. MAAs will consider issues such as resilience, accessibility, recognition, and cascading effects when evaluating vulnerabilities. The CJCS, in relation to the MAAP, will:

1. Include both the collection of self-assessment/inspection results and MAA execution.

2. Integrate assessments of all MA-related programs and activities to reduce redundancy and provide a more complete risk picture.

3. Develop and use established benchmarks and standards that focus upon identifying risk to mission, rather than solely policy compliance. OSD leads for MA-related programs and activities will provide SMEs to support CJCS development of benchmarks and standards that meet the needs of their program or activity.

4. Ensure assessments meet established periodicity requirements.

5. Oversee DTRA-led MAAs for DCAs and other MACB-prioritized DCI.

6. Establish an assessment implementation process.

7. See that assessment results are posted to the MA system of record.

8. Brief any MAA-identified high-risk finding for DCAs or other MACB-prioritized DCI to the MACB within 90 days of the completed assessment report.

(b) The DTRA MAA process will include:

1. Analysis on the resilience of the asset and the site's supporting commercial infrastructure with specific identification of:

a. Single points of service that, if exploited, would cause degradation of the asset's ability to meet mission requirements.

b. Those nodes susceptible to degradation to the asset's mission performance.

2. Adversarial approach analysis to evaluate the asset, site, and supporting infrastructure and to identify potential attack vectors to disrupt mission accomplishment.

3. Vulnerability analysis to identify vulnerabilities related to the critical capability, asset, and supporting infrastructure based upon the appropriate MA-related programs and activities and from the potential attack vectors provided by the adversarial approach analysis.

4. Enhanced cyber analysis to conduct on-network information and traffic collection to evaluate critical networks and control systems and to identify vulnerabilities and determine risk to mission execution.

a. Asset owners will coordinate with DTRA to grant ATC within 60 calendar days of the location's inclusion on the integrated assessment schedule. DTRA will report to the CJCS and DASD(DC&MA) any sites or assets for which owners are unable or unwilling to grant ATC. If within 30 calendar days of this notification the ATC is not granted, the DTRA-led MAA for that location will be cancelled.

b. Asset owners who desire an MAA without performing enhanced cyber analysis may request from the MA SSG co-chairs a formal waiver for this requirement.

c. Asset owners will provide DTRA with the latest MBRCA assessment results for all applicable TCAs and DCAs being assessed.

5. Analysis by the Defense Contract Management Agency's center of excellence for DIB supply chain network analysis, supporting the assessment with identification of critical industrial capabilities, foreign supplier dependencies, single or sole sources of supply, and associated industrial base risks (when applicable).

6. Analysis by Defense Information Systems Agency on vulnerabilities for networks and mission-essential long-haul communications.

7. Assessment team strategic risk assessment provided to the DASD(DC&MA), CJCS, and senior asset-owner leadership within 15 calendar days of completion of the assessment as well as a final report provided within 60 calendar days.

8. For DCAs and other MACB-prioritized DCI, availability of DTRA, DIA, and the appropriate centers of excellence to discuss their findings with the MACB and answer any additional questions.

(c) Appropriate Military Department and Defense Agency subordinate commands through their MA forums will perform required annual self-assessments or self-inspections from existing policy of MA-related program and activities. Self-assessment or self-inspection results will be shared with the MA system of record.

(d) The Military Departments and Defense Agencies will:

1. Resource a Military Department or Defense Agency MAA capability to meet assessment periodicity requirements for all TCAs and commands not covered by the DTRA MAAs.

2. Request assessment waivers from the CJCS.

3. Provide Military Department or Defense Agency augmentation to DTRA MAAs to ensure any additional MA equities for the Department or Agency are met.

4. Coordinate Military Department or Defense Agency MAA schedules and changes with the CJCS after conferring with appropriate CCMDs to ensure the assessment will not interfere with operational requirements.

5. Ensure subordinate commands perform yearly self-assessments or self-inspections and share results with the MA system of record.

6. Ensure Military Department or Defense Agency MAA assessors follow the CJCS-established assessment process.

7. Post results of Military Department or Defense Agency-led MAA of DCAs, Tier1 or 2 TCAs, and other MACB-prioritized DCI to the MA system of record and applicable DRRS.

8. Direct subordinate organizations operating in a tenant capacity on the installation of another DoD Component to participate in local MAA activities. Tenants will, at a minimum, provide mission requirements and dependencies for infrastructure mapping and resource planning.

9. Conduct MAAs at installations and sites in accordance with succeeding CJCS policy on MAAs (e.g., Joint Staff MAA Concept of Operations, April 2016).

10. Document and post to the MA system of record a risk assessment based on the threats, hazards, and vulnerabilities identified for each assessed DCA, Tier 1 or 2 TCA, or other MACB-prioritized DCI. The risk assessment, formulated, as per supplemental CJCS policy, through a measured analysis of risk factors, including asset criticality, threats and hazards, and vulnerabilities, will provide a record of the potential inability of the TCA to meet mission owner-established mission-essential capability conditions and standards as follows:

a. The TCA's potential inability to meet mission requirements chance is LOW.

b. The TCA's potential inability to meet mission requirements chance is MODERATE.

c. The TCA's potential inability to meet mission requirements chance is SIGNIFICANT.

d. The TCA's potential inability to meet mission requirements chance is HIGH.

11. The subordinate command's lead for readiness or planning will ensure risk assessments with significant or high potential failure conditions are also reported in DRRS.

(e) The CCMDs will:

1. Coordinate MAA schedules and changes with the CJCS and request assessment waivers from the CJCS.

2. Assist MAA executors in focusing assessment goals and support ATC requests through appropriate engagement with asset owners.

3. Provide subject matter expertise, when requested.

(4) The assessment process draws upon the expertise of all applicable MA-related programs and activities to achieve success. The MA forum structures at all levels should collaborate, assign leads for specific tasks based upon subject matter experience, and share results to further MA and individual program and activity goals.

b. Timeline and Result Application.

(1) Perform required self-assessments or self-inspections to meet existing policy requirements annually and share results with the MA system of record.

(2) A Joint or Military Department or Defense Agency-led MAA, with support from component SMEs and the local-level MA forum structure, will be performed:

(a) Every 3 years for locations housing DCAs or other MACB-prioritized DCI. DTRA MAAs will assess DCAs.

(b) Every 5 years for locations housing Tier 1 or select Tier 2 TCAs.

1. Select Tier 2 TCAs are those that are at the same locations as any DCA or Tier 1 TCA, or have been identified by a mission owner as a priority for assessment.

2. All other Tier 2 TCAs will be assessed no less often than every 7 years.

(c) For all other commands at the periodicity and at the discretion of the owning Military Department or Defense Agency or when requested by a CCMD.

(d) Newly designated DCAs will be scheduled for assessment during the development of the next annual MAAP schedule.

(e) The CJCS will produce a yearly MAAP schedule of all joint, Military Department, and Defense Agency MAAs to be conducted over the coming year.

1. The yearly MAAP schedule will identify all Tier 1 and 2 TCAs and DCAs to be assessed at each location.

2. MAAs will seek to assess all TCAs and DCAs at each location to reduce repeat assessments. For locations with numerous TCAs, the CJCS may waive this requirement, provided that all Tier 1 and 2 TCAs and DCAs at the location are still assessed in accordance with the 3, 5, or 7-year requirements listed under Paragraph 3.5.b.(2)(b).

c. MA Alignment to Annual Joint Assessment.

(1) CJCS Manual 3105.01 establishes a complementary process for the CJCS to assess annually strategic risk to U.S. interests identified in the National Defense Strategy and military risks in carrying out missions called for in the National Military Strategy. Mission owners with Tier 1 and Tier 2 TCAs assessed at significant or high risk will inform their annual joint assessment submissions with results from the MAA.

(2) The mission owner's survey response and supporting documentation will be posted to the MA system of record annually after the survey is submitted.

(3) Submissions will fall into the following categories based upon the mission owner's strategic mission.

(a) Operational Risk. This area defines risk to current military objectives as described in current, planned, or contingency operations. CCMDs will assess and report operational risk related to campaign plans, OPLANs, and CONPLANs.

(b) Force Management Risk. This area defines risks of sufficiently trained, equipped, and ready forces to meet operational requirements. Military Departments will assess and report force management risk related to their Title 10, United States Code, responsibilities.

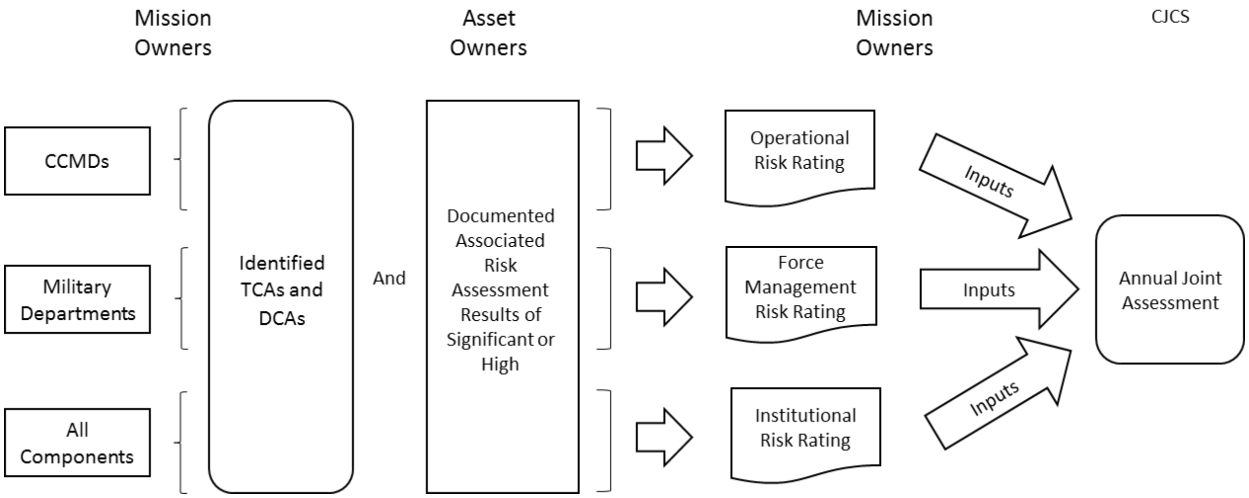
(c) Institutional Risk. This area defines risks to organizational, operational, and process effectiveness in improving national defense. OSD and DoD Components will assess and report institutional risk related to their MEFs.

(d) Future Challenges Risk. This area defines risks to future objectives, capabilities, or capacities to address anticipated threats. These risks are addressed through the weapon system acquisition, reliability, and force management processes where the MA community works with other governance structures established to deal with these issues.

(4) The CJCS will consider all MA-related survey results when completing the Chairman's Risk Assessment and Joint Military Net Assessment.

(5) Components will review the annual joint assessment input from their respective organizations to ensure feedback reflects MA equities and that MA efforts appropriately consider other concern areas raised.

Figure 5: MA Inputs to the Annual Joint Assessment



3.5. RISK MANAGEMENT PROCESS.

a. Method.

(1) The goal of the MA risk management process is to identify and implement solutions to achieve a level of acceptable risk by mission owners based on a thorough understanding of the limits on DoD resources.

(a) DoD implements risk management by building redundancy, improving the day-to-day resilience of essential capabilities, or identifying the means to restore essential capabilities quickly after a debilitating event occurs.

(b) Risk acceptance is also an option when made by the appropriate authority and shared with all stakeholders.

(c) At a minimum, DoD Components must make and share risk management decisions, including risk acceptance, on all Tier 1 and 2 TCAs with risks assessed as significant or high. Where possible, DoD Components should strive to reduce risk levels to moderate or lower.

(d) SecDef will be the risk management and risk acceptance authority for DCAs and MACB-prioritized DCI through the MACB.

(2) MA risk management consists of the elements of risk acceptance, building redundancy, or reduction of risk through mitigation or remediation.

(a) Mitigation focuses upon planning preventative actions to be taken in response to a warning or after an incident occurs to restore the essential capability rapidly. It includes both asset mitigation planning to return critical assets to operational status, such as prepositioned rapid runway repair material, and contingency planning by mission owners devising alternative methods to continue mission execution, such as transferring assets from other essential capabilities or missions.

1. At subordinate command levels, the MA forum structure will develop and regularly exercise continuity and restoration plans for all TCAs and DCAs under their authority.

2. MA forum structures of component-level mission owners will collaborate to develop MMPs to reconstitute essential capabilities and continue mission execution. Once developed, these plans will be recorded in appropriate campaign plans, OPLANs, CONPLANs, or component continuity plans for understanding and immediate reference. Appendix 15 of Annex C of an OPLAN or CONPLAN can be used to record these plans. Mission owners should review and exercise these plans regularly for familiarity.

(b) Remediation focuses planning upon corrective actions to known vulnerabilities of TCAs and DCAs by enhancing the security, protection, operations, resiliency, or redundancy to improve essential capability resilience.

1. At subordinate command levels, appropriate members of the MA forum structure will identify ways to address each identified vulnerability. The MA forum members will evaluate through the full scope of options (doctrine, organization, training, materiel, leadership, personnel, and facilities) for solutions in support of the JCIDS and PPBE processes. Subordinate commanders will record risk management decisions to remediate risk to these vulnerabilities and provide timelines for completion of associated actions. Any unresolved vulnerabilities will be elevated through the appropriate chains of command for resolution. Subordinate commanders will post local-level remediation plans to the MA system of record.

2. Component-level asset owners will review, revise, and approve local-level remediation plans and provide any additional risk management decisions and timelines for actions to address any unresolved risks. At a minimum, component-level remediation plans must provide the component's remediation position for all vulnerabilities related to any Tier 1 or Tier 2 TCA assessed at significant or high risk. For DCAs, DoD Component-level asset owners will provide risk-reduction recommendations to the MACB to develop remediation courses of action, including recommendations for SecDef decision if required. These will, at a minimum, address the recommended actions to be taken, the timeline to implement and complete these actions, and how these actions will change the level of assessed risk. Asset owner component level remediation plans will be posted to the MA system of record.

(3) Mission owners will provide their priorities for remediation and work with appropriate component-level asset owners to reach an acceptable level of risk. If unable to reach an acceptable consensus by both parties, components may refer these unresolved risk issues to the MACB for action.

(4) Risk reduction for DCAs and other MACB-prioritized DCI will include:

(a) Within 90 calendar days of DCA designation:

1. All mission owners who rely upon the asset will submit an MMP to the CJCS.

2. The appropriate Military Department, Defense Agency, Joint Staff, or OSD Component will submit to the CJCS any current plans for building redundancy to the capability the asset provides, the timeline for implementing this redundancy, and if the effort is funded.

(b) Within 15 calendar days of completing an assessment on the DCA or MACB-prioritized DCI, DTRA will submit the assessment's strategic risk findings to the DASD(DC&MA) and CJCS along with the asset owner. DTRA will complete its final report and submit to the appropriate mission and assets owners within 60 calendar days of the assessment.

(c) Within 15 calendar days of receiving the strategic findings, the DASD(DC&MA) and CJCS will identify a list of associated strategic issues to be addressed by the MACB.

(d) Initial MA SSG stage. Within 45-90 calendar days of completion of the MAA:

1. The MA SSG will convene in person or through the formal tasking process for the initial discussion to approve the list of strategic issues and designate a DoD Component lead for this effort.

2. Mission and asset owners should address the identified strategic risks and vulnerabilities as soon as received and should not wait until the MA SSG is convened.

3. The USD(C)/CFO, USD(A&S), and appropriate Military Department or Service officials should identify potential funding options for strategic issues identified for further research.

(e) MA SSG In-Process Review. Within 120 calendar days of the initial MA SSG discussion on the assessment, the MA SSG will reconvene to review progress on addressing the strategic issues identified. This discussion will review options considered, resources or additional assistance required to implement, expected timelines to execute the COAs, and any remaining concerns.

(f) MA SSG Assessment Close Out. Within 120 calendar days of the MA SSG's In-Process Review of the assessment, the MA SSG will reconvene to close out the assessment by providing completed or planned and budgeted actions for resolved strategic issues, or COAs for unresolved strategic issues that require SecDef decision. The MA SSG will review the completed actions and COAs and decide which of the following courses of action is warranted:

1. Return to DoD Component. The MA SSG decides that additional action at the DoD Component level is required and provides a timeline for completing these actions. This assessment will require an additional Close Out MA SSG discussion to complete this phase of the risk-management process.

2. Forward for Decision. The MA SSG co-chairs will forward completed actions and COAs to the MA ESG for recommendation to SecDef for decision. The MA ESG co-chairs will schedule the MA ESG to convene on this subject.

3. Forward for Awareness. The MA SSG co-chairs will forward completed actions that have sufficiently addressed the strategic risk issues to the MA ESG and SecDef for information only.

(g) MA ESG Convened. Within 90 calendar days of the MA SSG deciding that the strategic issues should be forwarded for decision, the MA ESG will convene to review the completed actions and COAs provided to address the strategic risk issues, and decide on one of the following actions:

1. Return the issue to specified DoD Components for further action. The MA ESG will define the tasks required and the timeline for accomplishment and reporting back to the MA ESG.

2. Forward the completed actions and COAs, along with MA ESG recommendations, via an action memorandum to SecDef for decision.

(h) SecDef Decision or Update. Within 60 calendar days of the MA SSG deciding to forward issues for awareness or the MA ESG deciding to forward issues for decision, an appropriate memorandum, information or action, will be drafted by the DASD(DC&MA) and CJCS, appropriately coordinated with the MA ESG members, and forwarded to SecDef.

(5) A single MA SSG or MA ESG meeting may be used to address multiple assessments at different stages of the process (e.g., one in initial stage, two in the in-process stage, and one in the close out stage.). The DASD(DC&MA) and the CJCS control scheduling of subjects for each MA SSG and MA ESG.

(6) The MA SSG and MA ESG will also develop departmental responses to emerging risks from evolving threats within the various MA-related programs and activities and provide courses of action to the SecDef.

b. Timeline and Result Application.

(1) Risk management is a continuous activity at all levels of command. For DCAs and MACB-prioritized DCI, components will meet the following timelines.

(a) Appropriate mission owners will develop MMPs for essential capabilities within 90 days of DCA designation or when the MACB prioritizes the essential capability for analysis.

(b) Asset owners will implement or propose risk-reduction recommendations for DCAs and other MACB-prioritized DCI vulnerabilities to support the in-process review MA SSG for that assessment.

(c) Designated DoD Components will implement or propose COAs to address assigned strategic risk issues to support the MA SSG's In-Process Review for that assessment.

(2) Mission owners and asset owners will collaborate on identified risks to essential capabilities and use existing tools such as planning updates, the issue paper, and the PPBE

process to reach an acceptable level of risk to the mission owner. Mission owners or asset owners may refer an issue of unacceptable and unresolved risk to the MA SSG at any time.

(3) RMPs for essential capabilities supported by DCAs and MACB-prioritized DCI will be presented to the MA SSG within 1 year of being identified or prioritized, or sooner if there is any significant increase in risk that requires immediate action.

(a) The MA SSG and MA ESG will forward these RMPs along with COA recommendations to the SecDef through appropriate channels for final decision, if required.

(b) Mission and asset owners will annually update the MA SSG on RMP action execution.

3.6. MONITORING PROCESS.

a. Method.

(1) The goal of the MA monitoring process is for all DoD Components and Principal Staff Assistants to maintain situational awareness on the risks related to their strategic missions. The monitoring process consists of threat monitoring, operational reporting, risk management implementation tracking, and development of the MA system of record to support monitoring activities.

(2) The MA Construct will include the following threat monitoring activities:

(a) Using existing reporting structures, CCMDs with geographic areas of responsibility will advise all appropriate DoD Components of changes to the threat picture in their AORs and post these alerts to the MA system of record. Additionally:

(b) USSPACECOM will similarly advise on space threat changes and post these alerts to the MA system of record.

(c) USCYBERCOM will similarly advise on cyber threat changes and synchronize and direct updates to the MA system of record.

(3) The MA Construct will include the following operational reporting actions:

(a) The CJCS will develop reporting requirements for Tier 1 and Tier 2 TCAs and DCAs using existing operational reporting to account for changes in operational status and situational reporting including daily status reporting during exercises and contingencies.

(b) Asset owners will follow CJCS reporting requirements.

(c) Mission owners will supplement operational asset owner reporting on Tier 1 and Tier 2 TCAs and DCAs by forwarding to the CJCS and all appropriate DoD Components the mission impact of TCAs and DCAs operational status changes and implementation of MMPs. This process will follow reporting procedures established by the CJCS.

(4) The MA Construct will include the following risk management implementation tracking actions:

(a) Asset owners will inform all appropriate DoD Components of changes or delays for risk reduction activities posted on the MA system of record.

(b) Asset owners will annually report to the MA SSG on the status of execution of RMP actions.

(5) An MA system of record will support MA Construct implementation.

(a) Designated by the CJCS, and managed by the Director, DTRA, the MA system of record will, in accordance with applicable law, incorporate data from multiple MA information databases and data feeds from DoD and appropriate U.S. Government departments and agencies to provide senior leaders at all levels within DoD a unified picture of risk and risk management actions.

(b) The MA system of record will include:

1. A common database for the sharing of mission and assets risk information.

2. Identification and visualization of the physical and cyber threats identified through the MAA process.

3. Cybersecurity activities and network operational status.

4. Status and availability of Tier 1 and Tier 2 TCAs and DCAs.

(c) Operation of the MA system of record will ensure proper classification of data and need-to-know requirements are met by users based upon published DoD security classification guidance.

(d) Director, DTRA, will design the MA system of record by integrating or replacing existing systems and applications to provide a unified capability to the Department.

b. Timeline.

(1) Monitoring is a continuous process for all DoD Components.

(2) Threat monitoring and operational reporting will adhere to the timelines established by supplemental CJCS policy.

(3) Asset owners will inform all appropriate DoD Components of changes or delays to risk reduction activities within 30 days of becoming aware of the change. Asset owners will provide a yearly update on the execution of risk reduction actions related to DCAs and MACB-prioritized DCI.

3.7. MA-RELATED PROGRAM AND ACTIVITY INTEGRATION

a. Aligning MA-Related Programs and Activities to Build Strategic Mission Resilience.

(1) The designated OPR for each MA-related program and activity will update its associated policy to align and support the goals of MA in improving the resilience of the execution of strategic missions, including development of individual benchmarks and standards for assessment.

(2) Each MA-related program or activity provides vital security, protection, or risk management expertise or results that further the goals of MA.

(a) Adaptive Planning, in accordance with CJCS Instruction 3100.01C, requires conducting an assessment of strategic and military risks. This includes providing the Chairman's assessment to Congress on the nature and magnitude of the strategic and military risks associated with executing the missions called for under the current national military strategy. High or significant risks for Tier 1 and 2 TCAs and DCAs identified during the MAA process may inform development of the Chairman's Risk Assessment.

(b) Regarding AT, Volume 1 of DoDI O-2000.16 directs the Department to establish, implement, and maintain a comprehensive AT program using an integrated systems approach designed to protect DoD elements and personnel from terrorist attacks. AT efforts support the MA Construct during each process to ensure the threat of terrorism is considered and accounted for during the execution of strategic missions.

(c) CBRN survivability efforts, in accordance with DoDI 3150.09, identify mission-critical systems and specify the subsets that must survive and operate in CBRN environments. MA and CBRN survivability are mutually supportive to ensure appropriate CBRN survivability protective measures for critical systems and assets that support strategic mission execution exist. These are regularly assessed, and protections are properly considered during the acquisition process for replacement capabilities.

(d) CBRNE preparedness, in accordance with DoDI 3020.52, ensures DoD Components identify processes, procedures, and actions specific to a CBRNE incident so that installation personnel, first responders and receivers, and the base populace are adequately prepared for a CBRNE incident. CBRNE protection efforts support the MA Construct during each process to ensure the threat from CBRNE incidents is considered and accounted for during the execution of strategic missions.

(e) COOP, in accordance with DoDD 3020.26, ensures the continuation of current approved DoD and DoD Component MEFs under all circumstances across the spectrum of threats. This effort supports MA by establishing the requirement for DoD Component MEFs and building continuity of operations plans to ensure mission accomplishment.

(f) Cybersecurity efforts, in accordance with DoDI 8500.01 and DoDI 5200.44, implement a multi-tiered cybersecurity risk-management process, including supply chain risk management for cyber-related components and services, to protect U.S. interests, DoD operational capabilities, and DoD individuals, organizations, information, and assets. MA leverages cybersecurity during each MA Construct process to identify, assess, and manage cyber-related risks that endanger strategic mission execution.

(g) DCI manages the risk to DoD's critical infrastructure. DCI fully supports MA by identifying TCAs and DCAs and managing the risks from supporting infrastructure.

(h) The Defense Security Enterprise, in accordance with DoDD 5200.43 and the guiding policy documents of each of its security programs, recognizes security is a mission-critical function of DoD. Its proper execution has a direct impact on all DoD missions and capabilities and on the national defense. The Defense Security Enterprise aligns with MA to ensure appropriate security safeguards exist in each of the appropriate security disciplines (e.g., physical, operational, industrial) to support strategic mission execution.

(i) Emergency management, in accordance with DoDI 6055.17, maintains DoD readiness and sustains MA by establishing and maintaining a comprehensive, all-hazards EM program. MA leverages the work of EM to assess, risk manage, and monitor threats and hazards that endanger strategic mission execution.

(j) Energy resilience efforts, in accordance with DoDI 4170.11, ensure readiness and sustainability policies and installation missions are considered and facilitated as part of installation energy management practices. This effort supports MA by addressing energy-related risks to strategic mission execution.

(k) Fire protection and prevention, in accordance with DoDI 6055.06, enhance DoD mission capabilities by protecting the U.S. homeland and critical bases of operation through preventive risk management, education, emergency response, and risk communication as they relates to fire. MA leverages this effort to assess and address risks from fire that endanger strategic mission execution.

(l) Regarding force health protection, DoDD 6200.04 directs commanders, supervisors, individual Service members, and the Military Health System to promote, improve, conserve, and restore the physical and mental wellbeing of members of the Armed Forces across the full range of military activities and operations. This effort supports MA by identifying and addressing health-related issues that endanger strategic mission execution.

(m) Insider threat efforts, in accordance with DoDD 5205.16, seek to prevent, deter, detect, and mitigate the threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of DoD resources or capabilities. MA leverages insider threat efforts during the assessment, risk management, and monitoring processes and seeks to prevent, deter, detect, and mitigate such threats that endanger strategic mission execution.

(n) LE, or suspicious activity reporting, in accordance with DoDI 2000.26, identifies persons involved in terrorism, criminal-related activities, and threats directed against DoD. MA leverages these efforts during the assessment and monitoring processes to highlight threats to strategic mission execution.

(o) Munitions operations risk management, in accordance with DoDD 6055.09E, protects people and property from the unintentional, potentially damaging effects of DoD military munitions. MA leverages these efforts during the assessment and risk management process to identify and address safety issues related to military munitions that could endanger strategic mission execution.

(p) Operational energy, in accordance with DoDD 4180.01, assesses and manages energy-related risks to operations, training, and testing, including assets, supporting infrastructure, equipment, supplies, platforms, and personnel. Operational energy supports MA by focusing on identifying and resolving energy-related risks that endanger strategic mission execution.

(q) Readiness Reporting, pursuant to DoDD 7730.65, provides a means to manage and report the readiness of DoD and its subordinate components to execute the national military strategy. MA leverages readiness reporting to assess the military's readiness to execute strategic missions and highlight and address high or significant risks.

(3) At command structures below the component level, representatives from these various programs and efforts will collaborate through their MA forums to identify, assess, manage, and monitor the risks to strategic mission execution.

b. MA Construct Examples.

Table 1 lists some expected activities by each of the individual MA-related programs and activities. Components may modify or add to these listed tasks as required by the organization structure of their component.

Table 1: MA Related Program or Activity Responsibilities

MA related program or activity	Identification Process: *Identify essential capabilities, critical systems, and critical assets*	Assessment Process: *Assess risk to essential capabilities*	Risk Management Process: *Evaluate risk reduction methods*	Monitor Process: *Maintain awareness of readiness and risk management execution*
Adaptive Planning	• Decompose campaign plans, OPLANs, CONPLANs to essential capabilities.	• Exercise essential capabilities to identify risks. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop mission mitigation plans for essential capabilities with significant or high risks.	• Execute mitigation plans, as required.
AT	• Ensure systems and assets covered by the AT program are analyzed and accounted for on the DCI list, as appropriate. • Account for TCAs and DCAs in AT program activities.	• Identify program-related risks to essential capabilities. • Develop Threat aspect of AHTA. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the AT program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the AT program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection. • Respond to changes in threat levels.

Table 1: MA-Related Program or Activity Responsibilities, Continued

MA-related program or activity	Identification Process: *Identify essential capabilities, critical systems, and critical assets*	Assessment Process: *Assess risk to essential capabilities*	Risk Management Process: *Evaluate risk reduction methods*	Monitor Process: *Maintain awareness of readiness and risk management execution*
CBRN Survivability	• Ensure systems and assets covered by the CBRN program are analyzed and accounted for on the DCI list, as appropriate. • Account for TCAs and DCAs in CBRN program activities.	• Identify CBRN program-related risks to essential capabilities. • Submit all program-specific assessments to the MAA-coordinator or post directly to the MA system of record. • Ensure annual CBRN Mission Critical Reports are posted in the MA system of record.	• Develop risk management options for risks related to the CBRN program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the CBRN program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.
CBRNE Preparedness	• Ensure systems and assets covered by the CBRNE program are analyzed and accounted for on the DCI list, as appropriate. • Account for TCAs and DCAs in CBRNE program activities.	• Identify CBRNE program-related risks to essential capabilities. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the CBRNE program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the CBRNE program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.
Continuity of Operations	• Identify component-level MEFs. • Ensure systems and assets covered by the COOP program are analyzed and accounted for on the DCI list, as appropriate. • Account for TCAs and DCAs in COOP program activities.	• Identify COOP program-related risks to essential capabilities. • Exercise COOP plans for DCI to identify risks. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the COOP program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the COOP program. • Execute mitigation plans for DCI. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.

Table 1: MA-Related Program or Activity Responsibilities, Continued

MA-related program or activity	Identification Process: • *Identify essential capabilities, critical systems, and critical assets*	Assessment Process: • *Assess risk to essential capabilities*	Risk Management • Process: *Evaluate risk reduction methods*	Monitor Process: • *Maintain awareness of readiness and risk management execution*
Cybersecurity	• Ensure systems and assets covered by the cybersecurity program are analyzed and accounted for on the DCI list, as appropriate. • Account for TCAs and DCAs in cybersecurity program activities. • Identify Mission Relevant Terrain in cyberspace and ensure analysis is submitted to the MA System of Record.	• Identify cybersecurity program-related risks to essential capabilities. • Exercise non-cyber methods for achieving mission execution. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the cybersecurity program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the cybersecurity program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.
DCI	• Identify mission-critical systems and assets related to essential capabilities.	• Identify supporting infrastructure-related risks to essential capabilities. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to DCI. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to DCI. • Maintain awareness of DCI readiness. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.
Programs under the DSE	• Ensure systems and assets covered by these programs are analyzed and accounted for on the DCI list. • Account for TCAs and DCAs in these programs' activities.	• Identify program-related risks to essential capabilities. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to these programs. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to these programs. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.

Table 1: MA-Related Program or Activity Responsibilities, Continued

MA-related program or activity	Identification Process: • *Identify essential capabilities, critical systems, and critical assets*	Assessment Process: • *Assess risk to essential capabilities*	Risk Management Process: *Evaluate risk reduction methods*	Monitor Process: • *Maintain awareness of readiness and risk management execution*
EM	• Ensure systems and assets covered by the EM program are analyzed and accounted for on the DCI list. • Account for TCAs and DCAs in EM program activities.	• Identify EM program-related risks to essential capabilities. • Develop all-hazards aspect of AHTA. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the EM program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the EM program. • Exercise recovery plans for DCI and essential capabilities. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.
Energy Resilience	• Ensure systems and assets covered by the Energy Resilience program are analyzed and accounted for on the DCI list. • Account for TCAs and DCAs in Energy Resilience program activities.	• Identify program-related risks to essential capabilities. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record. • Identify the critical energy loads for Defense Critical Infrastructure.	• Develop risk management options for risks related to the Energy Resilience program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the Energy Resilience program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.
Fire Prevention and Protection	• Ensure systems and assets covered by the Fire Prevention program are analyzed and accounted for on the DCI list. • Account for TCAs and DCAs in Fire Prevention program activities.	• Identify Fire Prevention program-related risks to essential capabilities. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the Fire Prevention program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to Fire Prevention program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.

Table 1: MA-Related Program or Activity Responsibilities, Continued

MA-related program or activity	Identification Process: • *Identify essential capabilities, critical systems, and critical assets*	Assessment Process: • *Assess risk to essential capabilities*	Risk Management • Process: *Evaluate risk reduction methods*	Monitor Process: • *Maintain awareness of readiness and risk management execution*
Force Health Protection (FHP)	• Ensure systems and assets covered by the FHP program are analyzed and accounted for on the DCI list. • Account for TCAs and DCAs in FHP program activities.	• Identify FHP program-related risks to essential capabilities. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the FHP program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the FHP program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.
Insider Threat	• Account for TCAs and DCAs in Insider Threat program activities.	• Identify Insider Threat program-related risks to essential capabilities. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the Insider Threat program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the Insider Threat program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.
LE	• Account for TCAs and DCAs in LE program activities.	• Identify LE program-related risks to essential capabilities. • Assist in development of the threat portion of the AHTA. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the LE program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the LE program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.

Table 1: MA-Related Program or Activity Responsibilities, Continued

MA-related program or activity	Identification Process: • *Identify essential capabilities, critical systems, and critical assets*	Assessment Process: • *Assess risk to essential capabilities*	Risk Management • Process: *Evaluate risk reduction methods*	Monitor Process: • *Maintain awareness of readiness and risk management execution*
Munitions Operation Risk Management	• Ensure systems and assets covered by the munitions operations program are analyzed and accounted for on the DCI list. • Account for TCAs and DCAs in program activities.	• Identify program-related risks to essential capabilities. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.
Operational Energy	• Account for TCAs and DCAs in Operational Energy program activities.	• Identify Operational Energy program-related risks to essential capabilities. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the Operational Energy program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Track risk management activities related to the Operational Energy program. • Monitor program-related threat changes and provide appropriate alerts to enhance preparedness and protection.
Readiness Reporting	• Evaluate assigned METs supporting essential capabilities. • Account for TCAs and DCAs in readiness program activities.	• Identify readiness program-related risks to essential capabilities. • Submit all program-specific assessments to the MAA coordinator or post directly to the MA system of record.	• Develop risk management options for risks related to the readiness program. • Participate in MA forum activities to prioritize risk management options for decision makers.	• Ensure DRRS data accurately reflects all assigned mission of the command. • Track risk management activities related to the readiness program. • Maintain awareness of DCI readiness.

SECTION 4: RISK MANAGEMENT FOR NON-DOD OWNED ASSETS

4.1. OVERVIEW. Many of the assets DoD relies upon to execute its strategic missions are either owned or supported by entities outside of DoD. Accordingly, DoD Components may not be able to perform all phases of the MA Construct and associated responsibilities as they would for DoD-owned infrastructure. This section provides the minimum requirements for each process of the MA Construct as it relates to non-DoD systems and assets.

4.2. DEVIATIONS TO THE MA CONSTRUCT FOR COMMERCIAL OR FOREIGN GOVERNMENT-OWNED TCAS.

a. Identification Process Deviations.

(1) Mission owners, supported by asset owners and other designated lead agencies, will identify commercial and foreign-owned TCAs critical to their strategic missions. Because of the Department's limited ability to implement risk management of these assets, it is advisable that:

(a) Mission owners limit designating commercial or foreign government-owned TCAs to only those unique, stand-alone type assets that provide direct support to mission execution (e.g., a bridge, port, or airfield).

(b) Commercial or foreign government-owned assets that provide support to another TCA (e.g., power, water, communications) will be designated as supporting asset vulnerabilities rather than TCAs.

(2) Mission owners will record and maintain these TCAs in the MA system of record. At a minimum, those BEIs related to the name of the asset, its location, who the asset supports, and the mission impact statement must be recorded.

(3) The ASD(HD&HA) will share all applicable commercial and foreign-owned TCAs with the Department of Homeland Security and the Department of State.

b. Assessment Process Deviations

(1) Mission owners will produce AHTAs for all identified commercial and foreign-owned TCAs based on referring the DIA global baseline assessment and applicable AOR supplement issued by the CCMD with geographic area of responsibility and post the completed AHTA to the MA system of record.

(2) The ASD(HD&HA) will leverage the assessments by the Department of Homeland Security Protective Security Advisors, or other similar assessments, for commercial TCAs, as applicable, and post assessment results to the MA system of record while abiding by all appropriate classification, proprietary, contractual, and protected critical infrastructure information requirements.

(3) CCMDs with geographic areas of responsibility will work with the Department of State and host nations, as appropriate and to the greatest extent possible, to assess foreign-owned TCAs and post assessment results to the MA system of record while abiding by all appropriate classification, proprietary, contractual, and protected critical infrastructure information requirements.

(4) MAAs will record as vulnerabilities any commercial provided service (e.g., electric power, water, communications), especially single points of failure that could disrupt the performance of a designated TCA. These vulnerabilities will be part of the risk assessment for the associated assets and essential capabilities.

c. Risk Management Process Deviations

(1) Mission owners, to the greatest extent possible, will perform risk management activities for commercial and foreign-owned TCAs related to their missions.

(2) Mission owners, to the greatest extent possible, will document Departmental risk management decisions for all commercial and foreign-owned TCAs that create a risk categorized as high or significant and may refer these issues to the MA SSG.

d. Monitoring Process Deviations. To the greatest extent possible, CCMDs with geographic areas of responsibility will:

(1) Establish a monitoring process for all commercial and foreign-owned TCAs within their AOR.

(2) Report changes in commercial and foreign-owned TCAs operational status for assets in their AOR to all DoD Components with interest in the assets.

SECTION 5: DEPARTMENTAL GOVERNANCE

5.1. MACB

a. Purpose

(1) The MACB will be the principal Department-level advocacy forum for implementing the MA Construct. There will be three levels of MACB – the MA ESG, the MA SSG, and working groups, as required.

(2) The MACB will focus on establishing MA priorities, managing risk to identified DCAs and prioritized strategic missions, and addressing evolving threats elevated from the DoD Components and MA-related programs and activities.

b. MA ESG

(1) The MA ESG will be co-chaired by the ASD(HD&HA) and the Director, Joint Staff.

(2) Meetings will be attended by a designated Senior Executive Service, general officer, or flag officer representative at the three to four-star level and a supporting officer, both with a TOP SECRET Sensitive Compartmented Information clearance, from each of the OSD Under Secretaries, Military Departments, CCMDs, Cost Assessment and Program Evaluation office, Director of Administration and Management, National Guard Bureau, and Office of the General Counsel of the Department of Defense.

(3) The MA ESG will review the current risks to strategic missions and DCAs and provide courses of action recommendations to the SecDef through memorandum or inputs to the PPBE or JCIDS processes, as applicable. Courses of action will include options to reduce risk to an acceptable level and an option to build sufficient resiliency to eliminate associated critical assets.

c. MA SSG

(1) The MA SSG is composed of representatives at the one to two-star level from the same organizations that provide representatives for the MA ESG and with the same clearances.

(2) The co-chairs will be the Deputy Assistant Secretary of Defense for Defense Continuity and MA, and the Vice Director, Joint Staff.

(3) The MA SSG will meet at least quarterly, or as required, unless the co-chairs determine that there are no relevant issues to consider.

d. MACB Roles and Responsibilities:

(1) The co-chairs will:

(a) Establish MA priorities.

(b) Establish the agenda for, call, and preside over all MACB meetings.

(c) Upon consultation with other MACB members, designate chairs for working groups, as required.

(d) Invite other U.S. Government organizations to send representatives, as appropriate, to attend, observe, and contribute to meetings and activities.

(2) MACB members will:

(a) Designate organizational representatives to serve in the working and sub-working groups.

(b) Nominate agenda items, and provide staffed positions and recommendations.

(c) Review, assess, and recommend policies, processes, and procedures to enhance cross-component integration on security, resilience, and risk management-related efforts.

(d) Recommend actions to synchronize MA information-sharing policies and to comply with statutory requirements.

(e) Identify and recommend best practices and solutions to enhance critical capability readiness and resilience across the Department.

e. MACB Executive Secretary:

(1) The MACB Executive Secretary function will be executed by the MA Directorate under DASD(DC&MA), with the assistance of the Joint StaffJ36.

(2) The MACB Executive Secretary will be responsible for the following tasks in support of the MA ESG and MA SSG:

(a) Coordinate and publish the meeting agenda.

(b) Coordinate all administrative and logistic responsibilities for meetings.

(c) Compile, package, and distribute read-ahead materials.

(d) Track and report the status of formal action items.

(e) As directed, seek nominations for issues to address and gather studies, white papers, or other documentation on issues requiring resolution or attention.

(f) Draft summaries of conclusions and publish final reports.

(g) Forward items to other senior leadership forums when directed.

f. MACB Working Groups:

(1) All MACB working groups are intended to be temporary, unless specifically designated otherwise by the co-chairs.

(2) As issues arise, through consensus of the MACB, an organization will be designated to chair the working group.

(3) Working group members will be appointed by their respective organizations and will be functional experts at the GS 13-15/O4-O6 level. Contract support personnel may participate in working groups in support of appointed members.

(4) All working groups will report to and communicate with the MACB through their appointed working group chair who must be a government employee (preferably an O-6/GS-15).

(5) When consensus on the resolution of assigned tasks is not reached, the issue will be presented, along with several possible courses of action, to the next higher level MACB (e.g., a working group presents issues for resolution to the MA SSG, and the MA SSG presents issues to the MA ESG).

(6) Working group chairs will:

(a) Execute actions and maintain oversight of tasks as directed by the MACB co-chairs.

(b) Identify and request the participation of action officers as required.

(c) Ensure appropriate coordination with DoD Component representatives on agenda issues and recommendations to the MACB.

5.2. MACB ALIGNMENT WITH OTHER DOD ACTIVITIES

a. Departmental Established Bodies.

(1) The MACB will collaborate with appropriate standing departmental governance bodies before addressing strategic risk issues to prevent duplication of effort.

(2) The MACB will invite appropriate members of other departmental governance bodies to coordinate with or participate in strategic risk issue discussions.

b. Integration with Departmental Processes.

(1) The MACB will support strategic guidance priorities.

(2) The MACB will provide the SecDef with COA recommendations to accept, mitigate, or remediate strategic risk through the PPBE, acquisition, and JCIDS processes. This MACB action may include:

(a) Endorsement or opposition of a DoD Component-submitted issue paper.

(b) USD(P) or CJCS submission of an issue paper on behalf of the MACB.

(c) Inclusion of a tasking in the Defense Planning Guidance.

GLOSSARY

G.1. ACRONYMS.

AHTA	all-hazards threat assessment
AOR	area of responsibility
ASD(HD&HA)	Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs
AT	antiterrorism
ATC	authority-to-connect
BEI	baseline element of information
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear and high-yield explosive
CCMD	Combatant Command
CDRUSCYBERCOM	Commander, United States Cyber Command
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
COA	course of action
CONPLAN	concept plan
COOP	continuity of operations
DASD(DC&MA)	Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance
DCA	defense critical asset
DCI	defense critical infrastructure
DepSecDef	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DIB	defense industrial base
DISN	Defense Information System Network
DoDD	DoD directive
DoDI	DoD instruction
DRRS	Defense Readiness Reporting System
DRRS-S	Defense Readiness Reporting System-Strategic
DSE	Defense Security Enterprise
DTRA	Defense Threat Reduction Agency
EM	emergency management
FHP	force health protection
FVEY	FIVE EYES
GS	general schedule
JCIDS	Joint Capabilities Integration and Development System

JMET	joint mission-essential task
J36	Deputy Director Nuclear, Homeland Defense, and Current Operations
LE	law enforcement
MA	mission assurance
MAA	mission assurance assessment
MAAP	mission assurance assessment program
MACB	mission assurance coordination board
MA ESG	Mission Assurance Executive Steering Group
MA SSG	Mission Assurance Senior Steering Group
MEF	mission-essential function
MET	mission-essential task
METL	mission-essential task list
MHS	Military Health System
MMP	mission mitigation plan
MRT-C	mission relevant terrain - cyberspace
OCA	original classification authority
OPLAN	operational plan
OPR	office of primary responsibility
PPBE	Planning, Programing, Budgeting, and Execution
RMP	risk management plan
RRP	risk response plan
SecDef	Secretary of Defense
SME	subject matter expert
TA	task asset
TCA	task critical asset
UJTL	universal joint task list
USCYBERCOM	United States Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(C)/CFO	Under Secretary of Defense Comptroller/Chief Financial Officer, Department of Defense
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USSOCOM	United States Special Operations Command
USSPACECOM	United States Space Command

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

asset. Defined in DoDD 3020.40.

asset owner. The DoD Component or subcomponent with PPBE responsibility for a DoD asset, or organizations that own or operate a non-DoD asset.

capability execution analysis. Coordinated analysis performed below the component level that identifies systems and assets critical to the execution of missions assigned and recorded in applicable Defense Readiness Reporting Systems.

capability provider. DoD Components that furnish forces, materiel, and other assets or capabilities to a mission owner to execute a mission.

core JMET. For MA, a specified mission or task assigned to a Combatant Commander through the Unified Command Plan that is not covered by the command's campaign plan, OPLAN, or CONPLAN.

critical. The designation assigned to a capability, system, or asset that without which will significantly degrade or prevent execution of a supported strategic mission.

critical capability. Defined in Joint Publication 5.0.

DCA. Defined in DoDD 3020.40.

DCI. Defined in DoDD 3020.40.

DCI line of effort. Those selective actions under the MA Construct directly related to the risk management of DCI. This effort is asset-focused, whereas MA manages all risks to strategic missions, including those from DCI.

defense critical capability. Specific critical capability identified as essential to strategic mission success by mission owners and then designated by the MACB for end-to-end analysis.

defense critical mission. Any global, trans-regional, multi-domain, or multi-functional mission designated by the Secretary of Defense as vital to national security and critical to the execution of strategic priorities and plans.

DSE. Defined in DoDD 5200.43.

essential capability. A mission owner-defined ability necessary to execute a MET from a strategic mission. Mission owners, with support from appropriate capability providers, define essential capabilities during mission decomposition as tactical-level, Service or Defense Agency UJTL tasks linked to those strategic national, strategic theater, or operational UJTL METs necessary to execute their strategic mission.

globally integrated environment. The structure of capabilities, forces, basing, and alliances that create the ability to implement globally integrated operations around the world.

globally integrated operations. The operations of a globally postured Joint Force that is able to quickly combine capabilities with itself and mission partners across domains, echelons, geographic boundaries, and organizational affiliations to address emerging threats.

hazards. Defined in DoDI 6055.17.

infrastructure. Defined in DoDD 3020.40.

MA. Defined in DoDD 3020.40.

MAA. Defined in DoDD 3020.40.

MAAP. A CJCS-developed process for installation-level assessments that integrates information on mission dependencies, asset criticality, area-specific hazards and threats, and vulnerabilities that may exploit those hazards and threats. Once combined, this information presents a more comprehensive understanding of risks to mission that may be present at all levels of operations.

MA center of excellence. A recognized DoD organization within the MA community of interest that provides broad leadership, best practices, research, development, coordination, and support around a specific focus area to drive solution-oriented efficiencies, collaboration, and results that benefit the entire DoD enterprise.

MA Construct. The DoD-wide risk management approach that synchronizes and integrates aspects of multiple security, protection, and risk management efforts throughout DoD to manage the risk to the Department's strategic missions. The MA Construct is made up of four process: identification, assessment, risk management, and monitoring.

MA information.

Information (data and databases) pertaining to DoD execution of assigned missions derived from and supporting the designated MA security, protection, and risk management programs.

Information includes but is not limited to asset lists or subsets; asset BEIs; criticality data; threat and hazard information at the global, region, area, or installation and local level; assessment reports; RMPs; operational status reports; program resource information and reports; readiness reporting; program process plans; and MACB and MACB working group information.

Information may be in the form of electronic files or hard copies or be available on web-enabled applications and databases, geospatial products, or imagery and photos.

MEF. Defined in DoDD 3020.26.

MET. Defined in DoDD 7730.65.

MMP. Defined in DoDD 3020.40.

MRT-C. Cyber analysis that includes documenting devices, internal and external links, operating systems, services, applications, ports, protocols, hardware, software, and other technical aspects of a system required for the function of a critical asset.

OSD Component. One of the offices that comprise OSD whose principal reports directly to the SecDef or DepSecDef.

mission owner. Defined in DoDD 3020.40.

mitigation. Defined in DoDD 3020.40.

protection. Defined in the DoD Dictionary of Military and Associated Terms.

remediation. Defined in DoDD 3020.40.

resilience. Defined in DoDD 3100.10.

risk. Defined in DoDD 3020.40.

risk assessment. Defined in DoDD 3020.40.

risk management. Defined in DoDD 3020.40.

RMP. Defined in DoDD 3020.40.

RRP. The capability provider/asset owner's input to the RMP that describes those doctrine, organization, training, materiel, leadership, personnel, and facilities actions to be taken to reduce risk to an acceptable level and the timelines to implement these actions.

strategic mission (for MA). DoD Component-level MEFs, including, but not limited to, OSD Components, and CCMD Unified Command Plan assigned missions, responsibilities, and tasks including campaign plans, OPLANs, CONPLANs, and core JMETs.

TA. An asset that is directly used to support execution of one or more operations, tasks, activities, or METs.

TCA. Defined in DoDD 3020.40.

TCA Tier 1. An asset whose loss, incapacitation, or disruption would result in mission failure at the DoD Component level of a MET or essential capability aligned with strategic missions.

TCA Tier 2. An asset whose loss, incapacitation, or disruption would result in severe mission degradation at the DoD Component level of a MET or essential capability aligned to strategic missions.

TCA Tier 3. An asset not currently assigned to support a strategic mission, but will become a Tier 1 or Tier 2 TCA when designated by its parent component to support a strategic mission.

threat. Defined in DoDD 3020.40.

REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 3100.01C, "Joint Strategic Planning System," November 20, 2015

Chairman of the Joint Chiefs of Staff Manual 3105.01, "Joint Risk Analysis," October 14, 2016

DoD Directive 3020.26, "DoD Continuity Policy," February 14, 2018

DoD Directive 3020.40, "Mission Assurance (MA)," November 29, 2016, as amended

DoD Directive 3100.10, "Space Policy," October 18, 2012, as amended

DoD Directive 4180.01, "DoD Energy Policy," April 16, 2014, as amended

DoD Directive 5111.01, "Under Secretary of Defense for Policy (USD(P))," June 23, 2020

DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1, 2012, as amended

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

DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended

DoD Directive 6055.09E, "Explosives Safety Management (ESM)," November 18, 2016, as amended

DoD Directive 6200.04, "Force Health Protection (FHP)," October 9, 2004

DoD Directive 7730.65, "Department of Defense Readiness Reporting System (DRRS)," May 11, 2015, as amended

DoD Instruction O-2000.16, Volume 1, "(U) DoD Antiterrorism Program Implementation: DoD Antiterrorism Standards," November 17, 2016, as amended

DoD Instruction 2000.26, "DoD Use of the Federal Bureau of Investigation (FBI) eGuardian System," December 4, 2019

DoD Instruction 3020.52, "DoD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Preparedness Standards," May 18, 2012, as amended

DoD Instruction 3150.09, "The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy," April 8, 2015, as amended

DoD Instruction 4000.19, "Support Agreements," December 16, 2020

DoD Instruction 4170.11, "Installation Energy Management," December 11, 2009, as amended

DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020

DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended

DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)," September 9, 2014, as amended

DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended

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

DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011, as amended

DoD Instruction 6055.06, "DoD Fire and Emergency Services (F&ES) Program," October 3, 2019

DoD Instruction 6055.17, "DoD Emergency Management (EM) Program," February 13, 2017, as amended

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

DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014, as amended

Joint Publication 5.0, "Joint Planning," current edition

Joint Staff Mission Assurance Assessment Concept of Operations, April 2016

National Infrastructure Protection Plan, 2013[1]

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

Presidential Policy Directive-21, "Critical Infrastructure Security and Resilience," February 12, 2013

United States Code, Title 10

[1] The NIPP can be found at https://www.dhs.gov/national-infrastructure-protection-plan.