DoD Directive 3020.40

Mission Assurance (MA)

Originating Component:	Office of the Under Secretary of Defense for Policy
Effective: **Change 1 Effective:**	November 29, 2016 September 11, 2018
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Directive 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure," January 14, 2010
Approved by: **Change 1 Approved by:**	Robert O. Work, Deputy Secretary of Defense Michael L. Rhodes, Director of Administration, Office of the Chief Management Officer of the Department of Defense

Purpose: This issuance:

- Establishes policy and assigns responsibilities to meet the goals of refining, integrating, and synchronizing aspects of DoD security, protection, and risk-management programs that directly relate to mission execution as described in the DoD Mission Assurance Strategy and Mission Assurance Implementation Framework.
- Assigns responsibilities for execution of critical infrastructure roles assigned to DoD in Presidential Policy Directive (PPD)-21 and prescribed in DoD Instruction (DoDI) 5220.22. Ensures consistency with applicable provisions of the National Infrastructure Protection Plan and compliance with applicable provisions of Part 29 of Title 6, Code of Federal Regulations.
- Maintains a Defense Critical Infrastructure (DCI) line of effort within MA to sustain programming, resources, functions, and activities supporting those responsibilities formerly under the Defense Critical Infrastructure Program (DCIP).
- Establishes the Mission Assurance Coordination Board (MACB) structure to manage risk at the DoD level through the MA Senior Steering Group (MA SSG) and the MA Executive Steering Group (MA ESG)).
- Integrates MA with existing DoD risk-management efforts such as the Defense Planning Guidance and the Planning, Programming, Budgeting, and Execution process.
- Integrates MA-related responsibilities assigned in the DoD Cyber Strategy.

TABLE OF CONTENTS

TABLES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to 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 the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within DoD (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

a. DoD uses MA as a process to protect or ensure the continued function and resilience of capabilities and assets by refining, integrating, and synchronizing the aspects of the DoD security, protection, and risk-management programs that directly relate to mission execution.

b. DoD Components will prioritize MA efforts in support of fulfilling critical DoD strategic missions. These include DoD or OSD Component-level mission essential functions (MEFs) and CCMD execution of operation plans (OPLANs), concept plans (CONPLANs), and core joint mission-essential tasks (JMETs).

c. The synchronization of security, protection, and risk-management programs through MA will result in a more comprehensive understanding of risk to mission that will inform the infrastructure support to CCMD plan development.

d. DoD weapon system acquisition and reliability activities may fall outside the scope of MA, but require coordination with individual MA-related programs or activities as outlined in Table 1.

e. Certain specific intelligence assets and activities are outside the scope of MA. In these cases the DoD Component asset owners ensure that the MA process is followed for identifying, assessing, and addressing risk from infrastructure and networks that support these excluded assets. Unresolved risk issues will be elevated to the Under Secretary of Defense for Intelligence (USD(I)) for final determination.

f. DoD will continue, under the MA construct and policy, existing efforts to meet national and DCI requirements established by PPD-21. Existing Department-level Defense Critical Infrastructure Program policy will remain effective until integrated into, replaced, or rescinded by MA policy. DoD Components will maintain sufficient resources to meet DCI responsibilities for identifying, assessing, managing, and monitoring risk to critical infrastructure and align associated security, protection, and risk management efforts under an MA construct. DoD Components will sustain and continue to prioritize resources to implement MA decisions in a dynamic threat environment. This issuance assigns DoD-wide critical infrastructure analysis, formerly conducted by the Defense Sectors, to parent DoD Components; this includes analysis of DoD and non-DoD networks, assets, and associated dependencies to coordinate and assist other DoD Components' analysis efforts.

g. DoD Components will follow the guidance in this issuance in meeting MA goals. (See Section 3.) The goals for MA are:

(1) Identify and prioritize critical missions, capabilities, functions, systems, and supporting assets.

(2) Develop and implement a comprehensive and integrated MA risk-management construct.

(3) Use risk-informed decision making to optimize risk reduction solutions.

(4) Partner with non-DoD entities, as appropriate and as permitted by law, to reduce risk.

h. DoD Components will protect information on MA plans, programs, personnel, and assets in accordance with established policy.

i. Collection, retention, and dissemination of U.S. Person information by Defense Intelligence Components supporting DoD MA will be conducted in accordance with DoD 5240.1-R.

1.3. SUMMARY OF CHANGE 1. Change 1 updates organization symbols, definitions, and references.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). In addition to the responsibilities in Paragraph 2.8., the USD(P):

a. Serves as the Principal Staff Assistant (PSA) to the Secretary of Defense on MA.

b. Establishes the MA construct, including strategies, plans, policy, and standards.

c. Synchronizes MA across DoD. Coordinates the synchronization of aspects of DoD's various security, protection, and risk-management programs and efforts directly related to mission execution under the MA construct. Ensures that the MA construct is consistent with the all-hazards approach prescribed in PPD-21.

d. Prescribes policy for MA-related information sharing with other federal departments and agencies and, as appropriate, with: State, local, regional, territorial, and tribal entities; intergovernmental organizations (IGOs) and nongovernmental organizations (NGOs); the private sector; and foreign countries. Ensures that such information-sharing policy also conforms to DoD policy on information sharing and information safeguarding, and safeguards information from disclosure that could harm DoD operations or jeopardize information-safeguarding agreements. The USD(P) will share MA-related information outside DoD by:

(1) Coordinating DoD collaborative efforts with the Department of Homeland Security (DHS) in the national-level sector partnership organizations established by PPD-21 and the National Infrastructure Protection Plan.

(2) Coordinating inclusion of appropriate DCI in DHS national critical asset lists, subject to established security requirements.

(3) Reviewing DHS critical asset lists for potential DCI.

(4) Provide timely information to the Secretary of Homeland Security and the national critical infrastructure centers necessary to support cross-sector analysis and inform the situational awareness capability for critical infrastructure.

e. Serves as the principal DoD representative for MA-related matters with Congress; the Executive Office of the President; other federal departments and agencies; State, local, regional, territorial, and tribal entities; IGOs and NGOs; the private sector; foreign countries; and other national-level partnership mechanisms established by PPD-21 and the National Infrastructure Protection Plan. Coordinates issues concerning MA-related security, protection, and risk-management programs and efforts with appropriate PSA leads. Reviews appropriate non-DoD policy for MA equities.

f. Develops a DoD-wide process to assess and manage the risk to DoD Component-level MEFs, including OSD Components, and CCMD OPLANs, CONPLANs, and core JMETs.

g. Exercises responsibility for the DCI line of effort within MA and synchronizing, and integrating the following within the MA construct: DCI; antiterrorism; chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) preparedness; law enforcement suspicious activity reporting; and continuity of operations efforts responsibilities.

h. Oversees strategic-level MA risk-management activities, including:

(1) Maintaining and co-chairing the MACB forums to address mission-related security, protection, and risk-management issues.

(2) Identifying risk issues for additional analysis by MA working groups.

i. Supports other DoD missions related to MA and critical infrastructure assigned to the Secretary of Defense in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 and PPD-35.

j. Manages the sector-specific agency (SSA) responsibilities for the national Defense Industrial Base (DIB) sector, as assigned in PPD-21, on behalf of the Secretary of Defense, supported by appropriate DoD Components, and collaborates, as appropriate, with the private sector; other federal departments and agencies; State, local, regional, territorial, and tribal entities; Government Coordinating Councils, IGOs, and NGOs; and foreign countries. These responsibilities include:

(1) Coordinating matters pertaining to DIB SSA responsibilities with the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)); the USD(I); the Assistant Secretary of Defense for Health Affairs; and the DoD Chief Information Officer (DoD CIO).

(2) Consulting on DIB SSA matters, as appropriate, with other federal departments and agencies; State, local, regional, territorial, and tribal entities; the private sector; and foreign countries.

(3) Appointing DoD co-chairs of the national DIB Sector Government Coordinating Councils and the DIB Critical Infrastructure Partnership Advisory Council.

(4) Encouraging risk-management approaches by those outside DoD to mitigate the effects of attacks against, or the consequences of catastrophic failures of, non-DoD-owned DCI assets and systems.

(5) Providing to the Secretary of Homeland Security, on an annual basis, sector-specific critical infrastructure information.

k. Provides DoD representation to the appropriate national sector Government Coordinating Councils.

l. Ensures that the Principal Cyber Advisor to the Secretary of Defense:

(1) Oversees the development, synchronization, and integration of cyber capabilities, activities, and policy with MA, in coordination with the USD(A&S) and DoD CIO.

(2) Coordinates alignment of the MA process and departmental cyber capabilities, including establishing clear cyber defense priorities to ensure that key missions are provided the appropriate level of protection.

(3) Oversees the development and maintenance of a consolidated cyber list of critical missions, capabilities, functions, systems, and supporting assets as part of the DCI list and greater mission assurance asset list (MAAL) to be used as a basis for addressing MA cybersecurity priorities.

(4) Oversees the alignment of cyber assessments with MA assessments by the CJCS. Ensures that cyber vulnerabilities related to MEFs, OPLANs, and CONPLANs, and CCMD core JMETs are adequately addressed.

2.2. USD(A&S). In addition to the responsibilities in Paragraph 2.8., the USD(A&S):

a. Integrates MA goals and activities with acquisition, procurement, military construction, and installation guidance.

b. Applies MA processes to the DIB, as applicable.

c. Develops effective options to respond to risks that are posed by emerging vulnerabilities or threats, including cyber threats.

d. Establishes policy for implementing an installation-level, all-hazards assessment methodology aligned with PPD-21, and a scoring system across DoD to support standardized risk-management decisions.

e. Synchronizes and integrates MA with policy and efforts of:

(1) Chemical, biological, radiological, and nuclear (CBRN) survivability.

(2) Emergency management.

(3) Munitions operations risk management.

(4) Energy resilience.

(5) Operational energy.

(6) Fire protection and prevention.

(7) Climate change adaptation and resilience.

f. Furthers MA objectives, consistent with USD(A&S) authorities and responsibilities, by consulting with other DoD Components and, as appropriate, with the private sector; other federal departments and agencies; State, local, regional, territorial, and tribal entities; Government Coordinating Councils, IGOs, and NGOs; and foreign countries. Provides DoD representation to the appropriate national sector Government Coordinating Councils.

2.3. USD(I). In addition to the responsibilities in Paragraph 2.8., the USD(I):

a. Establishes policy and plans to direct and integrate intelligence, counterintelligence, and security support to MA activities and, as appropriate, the national DIB Sector Government Coordinating Council, pursuant to DoDI 5220.22.

b. Establishes policy for and advises on Defense Intelligence Enterprise (DIE) MA capabilities, priorities, assessments, and investments. Oversees DIE MA activities, in consultation with the Director of National Intelligence, pursuant to DoDI 3020.39.

c. Synchronizes and integrates Defense Security Enterprise and insider-threat policies and efforts with the MA construct.

d. Reviews unresolved risk issues elevated by DoD Component asset owners for those intelligence assets specified as outside the scope of MA.

2.4. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE. In addition to the responsibilities in Paragraph 2.8., the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense:

a. Provides guidance to the DoD Components for submitting and displaying MA-related resource requirements for risk management within budget submissions.

b. Updates and provides advice to MACB forums on MACB-prioritized investments .

2.5. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS. In addition to the responsibilities in Paragraph 2.8., the Under Secretary of Defense for Personnel and Readiness:

a. Synchronizes and integrates appropriate readiness reporting, law enforcement, and force health protection policy and efforts with the MA construct.

b. Provides DoD representation to the appropriate national sector Government Coordinating Councils.

c. Provides oversight and coordination to the DoD Components on MA matters pertaining to the DoD Military Health System.

2.6. DOD CIO. In addition to the responsibilities in Paragraph 2.8., the DoD CIO:

a. Leads, in coordination with the USD(P) and CJCS, the development, implementation, and management of an MA common operating picture that supports business needs, facilitates decision making, and improves information sharing.

b. Synchronizes and integrates cybersecurity and DIB cybersecurity policy and efforts with MA.

c. In coordination with the USD(P) and USD(A&S), develops resilient technical solutions to further MA-related DIB and interagency efforts, as appropriate.

d. Provides DoD representation to the appropriate national sector Government Coordinating Councils.

e. Reviews DHS critical assets lists for potential cyber DCI.

2.7. DOD COMPONENT HEADS. The DoD Component heads:

a. Assign a member of the Senior Executive Service, a general officer, or a flag officer as Component MA lead for integrating MA efforts across the Component.

b. Establish and resource an office of primary responsibility for MA that includes, or can coordinate with, the DCI line of effort. Provide sufficient authorities to accomplish assigned tasks, including MA process execution and security, protection, and risk-management efforts across the Component.

c. Maintain staffing and resource levels necessary to meet continuing DCI responsibilities under an MA construct.

d. Participate in MACB forums, as prescribed in Section 3, and:

(1) Identify to the appropriate MACB forums any strategic risks that endanger execution of MEFs or CCMD OPLANs, CONPLANs, and core JMETs.

(2) Provide participants to appropriate MA working groups.

e. Publish or update, as appropriate, subordinate Component policy to synchronize and integrate DoD security, protection, and risk-management programs and activities with the MA construct in accordance with this issuance. Include senior agency officials responsible for privacy in efforts to govern and oversee information sharing, in accordance with DoD Directive (DoDD) 5400.11 and appropriate Component policies.

f. Maintain and review MA-related security, protection, and risk-management data, and provide that data, as appropriate, to other DoD Component heads. Adhere to appropriate records management practices.

g. Implement the MA process to identify, assess, manage, and monitor the risk to missions, systems, and assets that support mission execution. As necessary, coordinate with other DoD Component heads and other federal departments and agencies and, as appropriate, consult with: State, local, regional, territorial, and tribal entities; the private sector; and foreign countries to implement the MA process. Ensure that the analysis is recorded on the MAAL and DCI list, as applicable.

h. Develop, report, and monitor threat and hazard assessments (in accordance with methodology developed by the USD(A&S)) and changes to the threat and hazard environment, and integrate assessment information into risk-assessment and risk-management activities. Ensure that MA-related intelligence requirements are included in Component intelligence-collection plans.

i. Monitor the results of MA assessments and risk-response actions.

j. At a minimum, and in coordination with appropriate DoD Component heads, develop all hazards-based risk-management plans (RMPs) for defense critical assets (DCAs) and, as requested, other MACB-prioritized DCI that the DoD Component serves as the mission owner.

k. Develop mission mitigation plans for DCI related to the Component's MEFs.

l. Conduct MA education, training, and outreach activities in accordance with goals, objectives, and standards established by the USD(P) and CJCS.

2.8. OSD COMPONENT HEADS. In addition to the responsibilities in Paragraph 2.7., the OSD Component heads:

a. Designate an MA office of primary responsibility to provide oversight, coordination, and guidance to MA activities. At a minimum, participate in MACB forums and:

(1) Identify to the appropriate MACB forums any strategic risks that endanger mission execution related to their portfolio.

(2) Assign participants to appropriate MA working groups.

b. Apply the MA process to analyze and manage risk to Component MEFs. Coordinate with the DoD Components to identify, analyze, and manage risk related to PSA portfolio areas and core competencies. Ensure that the analysis is recorded on the MAAL and DCI list, as applicable.

2.9. SECRETARIES OF THE MILITARY DEPARTMENTS; COMMANDER, U.S. SPECIAL OPERATIONS COMMAND; CHIEF, NATIONAL GUARD BUREAU; AND DIRECTORS OF THE DEFENSE AGENCIES AND DOD FIELD ACTIVITIES. In addition to the responsibilities in Paragraph 2.7., the Secretaries of the Military Departments; Commander, U.S. Special Operations Command; Chief, National Guard Bureau; and the Directors of the Defense Agencies and the DoD Field Activities:

a. Establish structures and processes to align MA-related programs and activities, including the identification and prioritization of DCI, at all levels, from DoD Component to installation and tenant, as appropriate

(1) Designate an MA officer with the necessary security clearance and authority for addressing security, protection, and risk-management issues as the MA lead.

(2) Ensure that all DoD tenant units on an installation or residing in separate Defense Agency-owned or commercial leased spaces, regardless of Military Department, Defense Agency, or DoD Field Activity affiliation, participate in applicable installation MA structures and processes.

b. Collect, analyze, and disseminate MA-related threat and hazard assessments and warnings, as appropriate, to subordinate elements, the DoD Components, and other authorized activities.

c. In support of the CJCS's integrated MA assessment program, and with the assistance of the appropriate DoD Component heads, conduct MA assessments on installations with DCI to identify the vulnerabilities and risk to mission execution. Document and provide the results to the appropriate DoD Component heads.

d. In supporting the responsibilities assigned by Paragraph 2.7.j., develop and provide appropriate input to mission owners for their RMPs and to the appropriate geographic CCMD for risk-management support.

e. Manage the risk of loss or degradation of DCI. Integrate priorities of the Combatant Commanders, the CJCS, and the USD(P) for risk reduction during the budget process. Prioritize resources to implement MA decisions.

(1) Provide risk-management actions and associated asset information to the geographic CCMD where the asset is located and to appropriate mission owners in accordance with CJCS requirements.

(2) Provide to appropriate mission owners the changes in operational status of DCI in accordance with CJCS requirements.

f. Exercise and evaluate MA-related mitigation and emergency response plans.

g. At a minimum, update the appropriate MACB forums on the execution of MA-related, risk-management decisions and investments at the end of the DoD Component's yearly budget process for DCAs and any other DCI associated with MACB-prioritized mission areas that the Component owns.

h. Establish MA goals, objectives, and standards, and conduct MA education, outreach, and training activities in accordance with the established DoD MA goals, objectives, and standards.

2.10. CJCS. In addition to the responsibilities in Paragraph 2.7., the CJCS:

a. Provides to the Secretary of Defense and the USD(P) operational impact risk analysis related to MA.

b. Facilitates, monitors, and assesses the accomplishment of MACB-established MA priorities and activities for DoD. Designates the MA system of record for the compilation, storage, validation, sharing, and monitoring of MA information.

c. Develops and oversees an MA assessment program, integrating the assessment requirements of the MA-related programs and activities in coordination with the other DoD Component heads. Maintains a catalog of completed and upcoming MA-related assessments.

d. Implements the RMP development process for DCAs in coordination with the appropriate OSD officials and the DoD Component heads who have operational interest with each asset.

e. Integrates MA functions and activities into joint planning, doctrine, operational reporting, exercises, and training.

f. Reviews CCMD MA-related policy and guidance; standards; procedures; training; implementation plans; threat and hazard monitoring and reporting; and mitigation plans.

g. Co-chairs MACB forums.

2.11. COMBATANT COMMANDERS. In addition to the responsibilities in Paragraph 2.7., the Combatant Commanders:

a. Synchronize MA through an integrated risk-management methodology across CCMD missions, policies, plans, and programs mitigating mission-execution risk from the full spectrum of threats and hazards to mission-critical capabilities, functions, and supporting assets.

b. Ensure that DoD is able to execute missions by preventing or mitigating the loss or degradation of DoD-owned DCI within their assigned areas of responsibility in coordination with the DoD asset owner and the other DoD Component heads.

c. Implement the MA process to identify, prioritize, assess, and manage risks to CCMD MEFs, OPLANs, CONPLANs, and designated core JMETs.

d. Collect, analyze, and evaluate threat and hazard incidents and events, and then disseminate necessary advisories and warnings to appropriate DoD Components, other authorized activities, and subordinate activities.

e. Develop mission mitigation plans for the loss of all identified DCI related to OPLANs, CONPLANs, or core JMETs, based on CCMD priorities.

f. At a minimum, develop RMPs for the CCMD's identified DCAs and other MACB-prioritized DCI. Coordinate with other CCMDs or other DoD Component heads, and consult with necessary Service components, the Department of State, other federal departments and agencies, host-nation officials, and the private sector, as necessary.

2.12. PSAS ASSIGNED POLICY RESPONSIBILITY FOR MA-RELATED PROGRAMS AND ACTIVITIES. PSAs assigned policy responsibility for MA-related programs and activities must update and maintain supporting guidance (see Table 1) to reflect alignment with the MA processes of identification, assessment, risk management, and status monitoring. These existing security, protection, and risk-management programs and activities will continue to meet

individually established goals and responsibilities that are operational and regulatory, and share the mission-based analysis and results related to the MA construct with other MA community members.

Table 1. MA-Related Programs and Activities

MA-related programs and activities include, but are not limited to:	
Programs/Activities	**Supporting Guidance**
Adaptive Planning	CJCS Instruction 3100.01C
Antiterrorism	DoDI O-2000.16
CBRN Survivability	DoDI 3150.09
CBRNE Preparedness	DoDI 3020.52
Continuity of Operations	DoDD 3020.26
Cybersecurity	DoDI 8500.01 and DoDI 5205.13
DCI	Contained in MA policy
Defense Security Enterprise. Composed of personnel, physical, industrial, information, and operational security programs; special access programs security policy; critical program information protection policy; and security training.	DoDD 5200.43
Emergency Management	DoDI 6055.17
Energy Resilience	DoDI 4170.11
Fire Prevention and Protection	DoDI 6055.06
Force Health Protection	DoDD 6200.04
Insider Threat	DoDD 5205.16

Table 1. MA-Related Programs and Activities, Continued

MA-related programs and activities include, but are not limited to:	
Programs/Activities	**Supporting Guidance**
Law Enforcement. Suspicious activity reporting.	DoDI 2000.26
Munitions Operations Risk Management	DoDD 6055.09E
Operational Energy	DoDD 4180.01
Readiness Reporting	DoDD 7730.65

SECTION 3: MEETING MA GOALS

3.1. MA GOALS 1 AND 2. To meet Goals 1 and 2 (see Paragraph 1.2.g.), the DoD Component heads and PSAs will:

a. Synchronize and integrate MA, and the fully incorporated DCI responsibilities listed in this issuance, with the existing security, protection, and risk-management programs and activities of antiterrorism; Defense Security Enterprise; law enforcement; emergency management; continuity of operations; CBRN survivability; force health protection; CBRNE preparedness; cybersecurity; operational energy; and energy resilience as they relate to execution of missions. MA will be further augmented by the efforts of readiness reporting, insider threat reporting, adaptive planning, munitions operations risk management, and other mission-related security, protection, and risk-management activities, as applicable, to provide senior leaders with increased visibility and knowledge of risk to assist them in decision making.

b. Ensure that critical mission owners determine the acceptable level of risk for their assigned missions.

3.2. MA GOAL 3. Accomplishing Goal 3 (Paragraph 1.2.g.) requires synchronization and integration of MA-related programs and activities at the tenant and installation level, DoD Component level, and DoD level to understand holistically the criticality to mission execution of assets and capabilities; the existing threats and hazards to, and vulnerabilities of, those assets and capabilities; and the best ways to complete the MA risk-management process to achieve an acceptable level of risk. To achieve this goal DoD will use MA forums as follows:

a. Installations and tenants will designate an MA office of primary responsibility to integrate and synchronize MA activities at the local level and elevate risk issues through their chains of command to appropriate DoD Component heads. Unit commanders or civilian managers and directors responsible for DoD elements occupying leased facility space, or space in buildings owned or operated by the U.S. General Services Administration not located on DoD property, will implement the MA construct to the greatest extent feasible.

b. The DoD Component heads will:

(1) Create an MA forum to address internal risk in ensuring achievement of Component MEFs.

(2) Address risk issues elevated from installations and tenants.

(3) Coordinate the management of CCMD-related mission execution risk.

(4) Elevate strategic risk issues to the appropriate MACB forums.

(5) Submit requirements and supporting resource requests in support of MA.

c. The MACB forums will prioritize, oversee, and coordinate DoD enterprise-level MA activities and address DoD strategic risk issues in coordination with other established governance bodies.

d. The MA SSG will publish and annually update a list of PSA and DoD Component MA OPRs to facilitate Military Department and Combatant Command efforts to effectively identify and address risk issues across the DoD.

e. The MA ESG, using the MACB structure, will submit risk reduction recommendations to the Secretary of Defense for decision.

f. The MA SSG will inform the DoD Components when the governing policy for MA-related programs and activities is being issued, updated, replaced, or rescinded.

3.3. MA GOAL 4. To meet Goal 4 (see Paragraph 1.2.g.), OSD and DoD Component heads will:

a. Coordinate on the risk management of strategic and operational missions with other federal departments and agencies, when appropriate.

b. Consult with State, local, regional, territorial, and tribal entities, as well as the private sector and foreign countries, when appropriate.

GLOSSARY

G.1. ACRONYMS.

CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high yield explosive
CCMD	Combatant Command
CJCS	Chairman of the Joint Chiefs of Staff
CONPLAN	concept plan
DCA	defense critical asset
DCI	defense critical infrastructure
DHS	Department of Homeland Security
DIB	defense industrial base
DoD CIO	Department of Defense Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
IGO	intergovernmental organization
JMET	joint mission-essential task
MA	mission assurance
MAAL	mission assurance asset list
MACB	mission assurance coordination board
MEF	mission essential function
NGO	nongovernmental organization
OPLAN	operation plan
PSA	Principal Staff Assistant
RMP	risk-management plan
SSA	sector-specific agency
SSG	Senior Steering Group
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

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

asset. A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations.

DCA. An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its missions.

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

Defense Security Enterprise. Defined in DoDD 5200.43.

energy resilience. Defined in DoDI 4170.11.

Government Coordinating Council. A council formed to enable interagency and cross-jurisdictional coordination. The Government Coordinating Councils are composed of representatives from across various levels of government (federal, State, local, or tribal) as appropriate to the operating landscape of each individual national sector.

hazards. Defined in DoDI 6055.17.

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

infrastructure. The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole.

integrate. The arrangement of efforts to reduce redundancy and operate as a whole.

MA. A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions in any operating environment or condition.

MA assessment. Assessment of the discipline under the mission assurance umbrella (antiterrorism; DCI; CBRNE preparedness; CBRN survivability; emergency management; cybersecurity; explosives safety; physical security; continuity of operations, force health protection) to identify vulnerabilities and gaps that could prevent accomplishment of a unit, installation, or higher authority mission.

MAAL. The composition of all assets required for mission execution. DCI is a subset of the MAAL.

MEF. Defined in DoDD 3020.26.

mission execution aspects. Requirements of DoD security, protection, and risk-management programs that identify and address risk to mission execution rather than administrative or programmatic needs.

mission mitigation plan. A plan developed by a mission owner that reflects how to respond to the loss or incapacitation of identified DCI.

mission owner. The OSD or DoD Component having responsibility for the execution of all or part of a mission assigned by statute or the Secretary of Defense.

mitigation. Actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure.

network. A group or system of interconnected or cooperating entities, normally characterized as nodes (assets), and the connections that link them.

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

operational energy. Defined in DoDI 4180.01.

remediation. Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified.

risk. Probability and severity of loss linked to threats or hazards and vulnerabilities.

risk assessment. A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks.

risk management. A process by which decision makers accept, reduce, or offset risk and subsequently make decisions that weigh overall risk against mission benefits. Risk management is composed of risk assessment and risk response.

risk response. Actions taken to remediate or mitigate risk or reconstitute capability in the event of loss or degradation.

RMP. A plan that describes the risks to a mission arising from an asset's operational factors and the decisions that balance risk cost with mission benefits.

SSA. Defined in PPD-21.

task critical asset. An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD or OSD Components to execute the capability or mission-essential task it supports. Task critical assets are used to identify defense critical assets.

tenant. Defined in DoDI 4000.19.

threat. An adversary having the intent, capability, and opportunity to cause loss or damage.

REFERENCES

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

Code of Federal Regulations, Title 6, Part 29

Department of Homeland Security, "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resiliency," 2013

DoD Cyber Strategy, April 2015

DoD 5240.1-R, "Procedures Governing the Activities of the DoD Intelligence Components that Affect United States Persons," December 7, 1982, as amended

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

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

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

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

DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014

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, "DoD Antiterrorism (AT) Program Implementation," November 17, 2016, as amended

DoD Instruction 2000.26, "Suspicious Activity Reporting (SAR)," September 23, 2014, as amended

DoD Instruction 3020.39, "Mission Assurance Policy for the Defense Intelligence Enterprise (DIE)," March 2, 2015, as amended

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," April 25, 2013, as amended

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

DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010, 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," December 21, 2006

DoD Instruction 6055.17, "DoD Emergency Management (EM) Program," February 23, 2017, as amended

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

DoD Mission Assurance Strategy, April 2012

DoD Mission Assurance Strategy Implementation Framework, October 2013

National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," January 8, 2008[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

Presidential Policy Directive 35, "U.S. Nuclear Weapons Command and Control, Safety, and Security," December 9, 2015

[1] Copies of this restricted distribution document are available to authorized personnel upon request to DHS.