



# Department of Defense DIRECTIVE

NUMBER 5160.54

January 20, 1998

---

---

USD(P)

SUBJECT: Critical Asset Assurance Program (CAAP)

- References:
- (a) DoD Directive 5160.54, "DoD Key Asset Protection Program (KAPP)," June 26, 1989 (hereby canceled)
  - (b) DoD Directive 3020.36, "Assignment of National Security Emergency Preparedness (NSEP) Responsibilities to Department of Defense Components," November 2, 1988
  - (c) DoD Directive S-3600.1, "Information Operations (IO) (U)," December 9, 1996
  - (d) DoD 5160.54-R, "Industrial Facilities Protection Regulation," March 1977, authorized by this Directive
  - (e) through (n), see enclosure 1

## 1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update DoD policies and responsibilities for the protection and assurance of DoD and non-DoD Critical Assets worldwide, to support the requirements of reference (b), and to implement the policies established by reference (c) as they pertain to Critical Assets that are, include, or depend upon Information Systems. (See definition E2.1.9.)

1.2. Expands the requirement to identify Critical Assets and assure their integrity, availability, survivability, and capability to support vital DoD missions across the full range of military operations.

1.3. Provides for an integrated infrastructure vulnerability assessment and assurance program based on an analysis of the identified Critical Assets using risk

management principles. The risk management-based analysis provides the information necessary to effectively allocate available resources necessary for assurance.

1.4. Continues the authorization to publish reference (d), and authorizes the publication of DoD 5160.54-M, consistent with DoD 5025.1-M (reference (e)).

## 2. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

## 3. DEFINITIONS

The terms used in this Directive are defined in enclosure 2.

## 4. POLICY

It is DoD policy to:

4.1. Identify and ensure the availability, integrity, survivability and adequacy of those assets, (domestic and foreign) whose capabilities are deemed critical to DoD Force Readiness and operations in peace, crisis, and war by providing for their protection from all hazards; mitigating the effect of their loss or disruption; and/or planning for timely restoral or recovery. The level of assurance appropriate for each asset is a risk management decision of the owning or controlling DoD Component, made in coordination with those dependent on the asset, and based on its criticality, the threat, and resources available.

4.2. Recognize that critical DoD equipment, facilities, and services are dependent upon non-DoD assets -- the international and national infrastructures, other facilities and services of the private sector, and those of other Government Departments and Agencies; and that non-DoD assets essential to the functioning of DoD Critical Assets are also Critical Assets of concern to the Department of Defense. Critical Assets include information systems and computer-based systems and networks that can be distributive in nature.

4.3. Recognize that in peacetime responsibility for protecting non-DoD Critical Assets and designing their security rests primarily with the civil sector owners and with local, State, and Federal law enforcement authorities and that responsibility for protecting non-U.S. Critical Assets rests with the appropriate national authority. However, the Department of Defense must participate with the civil sector, emergency preparedness and law enforcement authorities in planning for Critical Asset assurance during an emergency, and must be prepared, in concert with the appropriate authorities and within defense priorities, to assist in their protection during emergencies, including natural disaster, physical or technical attack, and technological or other emergency that seriously degrades or threatens DoD operations. (See DoD Directives 3025.1, 3025.12, and 3025.15, references (f) through (h).)

4.4. Provide an integrated asset and infrastructure vulnerability assessment and assurance program for the protection and assurance of DoD and non-DoD Critical Assets worldwide through the CAAP. The CAAP must provide a comprehensive and integrated decision support environment to represent the relationship between Critical Assets and force readiness and operations in peace, crisis or war that can be used to assess the dependencies, vulnerabilities and effects of the disruption or loss of Critical Assets or supporting infrastructures on their plans and operations. The CAAP must also provide the capability for Critical Asset assurance analysis, planning, prioritization, resource programming and response necessary to mitigate the disruption or loss of Critical Assets. It must also ensure that the collection, retention, and dissemination of CAAP information are in compliance with applicable U.S. law, statutes, directives, and policies as delineated by the established intelligence oversight program. See DoD Directive 5240.1 and DoD 5240.1-R (references (i) and (j)).

## 5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Policy shall:

5.1.1. Provide policy direction and guidance for the development and implementation of CAAP as an element of national security emergency preparedness.

5.1.2. Represent the Secretary of Defense with other Federal Departments and Agencies and with industry in the development, review, and approval of standards for the assurance of all Critical Assets and coordinate such agreements as may be appropriate for this program.

5.1.3. Develop and lead a process for annual program review of the CAAP

with the Components and the DoD Executive Agent that includes an analysis of the program effectiveness in meeting goals and objectives, an assessment of the performance of organizations in accomplishing their roles and responsibilities, a review of threats and technologies, and the status of planning and analysis for the assurance of Critical Assets to ensure compliance with this Directive.

5.1.4. Exercise classification authority for CAAP, and publish classification guidance.

5.1.5. Establish, support and provide the Co-Chair (with the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence) for the Critical Infrastructure Protection Working Group (CIPWG).

5.1.6. Maintain and revise this Directive.

5.2. The Under Secretary of Defense for Acquisition and Technology shall:

5.2.1. Comprehensively integrate the policies established by this Directive in acquisition policy guidance, to include the Federal Acquisition Regulations System (reference (k)); develop assurance standards; and ensure that internal and external infrastructure protection, mitigation, detection, reaction and recovery measures are designed into the acquisition process, systems being developed and acquired, and the supporting industrial base.

5.2.2. Foster research on infrastructure systems assurance and analysis and promote development of infrastructure interdependency analysis. Identify technologies that represent threats to Critical Assets or related infrastructures (e.g., information or command and control systems), countermeasures technologies for existing or emerging threats, and technologies that may have inherent susceptibilities or vulnerabilities.

5.2.3. Provide policy to assess and mitigate infrastructure dependencies and vulnerabilities of specific DoD installations, facilities and supporting private sector facilities and systems.

5.2.4. In accordance with instructions from the DoD Executive Agent, provide DoD installations and facilities database support to facilitate maintenance of Critical Assets data by the DoD Components for inclusion in the CAAP.

5.3. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

5.3.1. Integrate the policies established by this Directive into policy guidance and standards promulgated for functional areas assigned by DoD Directive 5137.1 (reference (l)). Ensure, in consultation with Under Secretary of Defense for Acquisition and Technology, infrastructure dependencies and protection, mitigation, detection, reaction and recovery measures are considered during command, control, communications, intelligence, information and security systems development and acquisition. Ensure that intelligence, counterintelligence, and security countermeasure programs support the protection, survivability, availability, integrity and recovery of Critical Assets.

5.3.2. Provide the Co-Chair (with the Office of the Under Secretary of Defense for Policy) for the CIPWG.

5.3.3. Require the Director, Defense Investigative Service (DIS), to:

5.3.3.1. Conduct, in coordination with the appropriate DoD Component and with permission of the owners, on-site surveys, to include vulnerability analyses to physical and technical threats, for each non-DoD Industrial and Infrastructure Critical Asset designated by the DoD Executive Agent as requiring on-site survey.

5.3.3.2. Maintain liaison with the DoD Executive Agent, the responsible DoD Component, and consult with industry, as appropriate. Develop CAAP survey procedures in coordination with the DoD Executive Agent, and support courses of instruction to orient and train Government and industry personnel on CAAP surveys. Obtain technical assistance from other Components, as required.

5.3.4. Require the Director, Defense Intelligence Agency (DIA), in coordination with the National Security Agency (NSA), the DIS, the Federal Bureau of Investigation (FBI), and the Director, Central Intelligence, to develop procedures for continuous analysis of the hostile intelligence; special operations; and technical, terrorist, criminal and other transnational threats to Critical Assets and Infrastructures; develop and maintain a Critical Asset and Infrastructure Threat Assessment, and advise the DoD Executive Agent, the Chairman of the Joint Chiefs of Staff and the DoD Components of hostile threats to Critical Assets and Infrastructures in their areas of responsibility as evolving threats become known. These activities must be accomplished within the provisions of DoD Directive 5240.1 and DoD 5240.1-R (references (i) and (j)).

5.3.5. Require the Director, National Imagery and Mapping Agency, to

support the DoD Executive Agent's requirements for imagery and maps needed for CAAP.

5.3.6. Require the Director, Defense Information Systems Agency, to:

5.3.6.1. Provide, in conjunction with the DoD Components, for the assurance of the Defense Information Infrastructure (DII) and mitigation of the effects of its loss or disruption.

5.3.6.2. Coordinate with the National Communication System (NCS) to identify National Information Infrastructure (NII) assets critical to the DoD operations and National Security and Emergency Preparedness telecommunications. Identify to the DoD Executive Agent and the appropriate DoD Components the Critical Assets of the DII and the NII whose disruption or loss would seriously affect DoD operations and the nature of those effects. Coordinate with the DoD Executive Agent, the DoD Components, and the NCS regarding actions taken to increase the reliability, redundancy, protection, and restoral of information systems supporting Critical Assets.

5.3.6.3. Provide for overall coordination of the Computer Emergency Response Team (CERT) activities of the DoD Components and their interface with CERT-related activities of the Federal Government (to include the FBI), the NSA for national security systems, and private sector.

5.4. The Chairman of the Joint Chiefs of Staff shall:

5.4.1. Ensure identification of Critical Assets necessary for the execution of Deliberate and Crisis Action Plans and plan for mitigation of their loss or disruption. Identify those Critical Assets to the DoD Executive Agent.

5.4.2. Ensure that disruption and loss of Critical Assets, to include supporting national infrastructures, are scripted and responded to in Joint Exercises.

5.5. The Secretary of the Army, as the DoD Executive Agent, shall:

5.5.1. Develop, implement and administer the CAAP to meet the requirements described in subsection 4.4., above. Obtain Critical Asset nominations from the DoD Components, integrate them into the CAAP, and program and provide CAAP resources for support of CAAP decision support systems, analytic and management activities. Provide the capability for each DoD Component to use the CAAP for identification, analysis and assurance of assets critical to its operations. In coordination with the DoD Components, establish priorities for infrastructure analysis

and remediation, recommend actions to the Components based upon the CAAP and DIA threat analysis, and review the CAAP annually with the Under Secretary of Defense, for Policy (USD(P)) and the Components.

5.5.2. Develop, publish and administer DoD 5160.54-R (reference (d)), and 5160.54-M, consistent with DoD 5025.1-M (reference (e)).

5.5.3. Coordinate with other Departments and Agencies, as required, to solicit nominations of Infrastructure Assets critical to national defense applications. Designate non-DoD Industrial and Infrastructure Critical Assets that require on-site surveys and vulnerability assessments. Coordinate with DIS regarding conduct of industrial Critical Asset site surveys and vulnerability assessments.

5.5.4. Ensure that regulations, plans, and procedures governing military support to law enforcement in civil disturbances, as promulgated under DoD Directive 3025.12 (reference (g)), facilitate response by the DoD Components to protect Critical Assets under any conditions or circumstances covered by that Directive.

5.6. The Secretary of the Navy shall require the Program Manager, Joint Program Office for Special Technology Countermeasures, to provide the infrastructure assurance analysis and vulnerability assessment support to the DoD Executive Agent.

5.7. The Heads of the DoD Components shall:

5.7.1. Identify those assets critical to their operations (to include the supporting DoD and non-DoD infrastructures and other civil sector facilities and services), nominate those Critical Assets for inclusion in the CAAP, conduct risk assessments, and designate their category of importance in accordance with the instructions of the DoD Executive Agent.

5.7.2. Retain overall responsibility for the assurance of the Critical Assets subject to their authority or control. Program and provide for increased Critical Asset reliability, security and redundancy; plan for their disruption or loss and subsequent restoral; and develop systems that are less dependent upon vulnerable infrastructures and systems. Program and provide for supplemental integrated infrastructure vulnerability assessment and assurance capability when requirements exceed organic capabilities. Provide for a CERT capability.

5.7.3. Include a contractual requirement for cooperation in vulnerability assessments and assurance planning when contracting for private sector facilities, services and products, and consider all-hazard assurance of service when awarding

contracts.

5.7.4. Review annually all Critical Asset nominations and recommend changes in accordance with the instructions of the DoD Executive Agent. Review the CAAP annually with the USD(P) and the DoD Executive Agent. Provide senior (flag or senior executive service) representation on the CIPWG.

5.7.5. Assign personnel to the Executive Agent to support the CAAP and comply with the requirements of the DoD Executive Agent in accordance with this Directive.

5.7.6. Require that commanders of DoD installations conduct an annual review with all tenant activities of all Critical Assets associated with their installation, to include supporting DoD and non-DoD infrastructures and other civil sector facilities and services upon which the Critical Assets depend. This review shall include the validation of data on facilities and their dependencies, an examination of Installation and tenants' plans for increasing reliability, reducing vulnerabilities, mitigating hazards to and the restoration of Critical Assets, and a review of these plans with the FBI, local emergency services personnel (including local law enforcement), the National Guard, and the representatives of critical infrastructure and support service providers, as appropriate. Assist tenant activities in direct coordination with local providers of critical infrastructure and other support services necessary to the operation of the their Critical Assets. Require that commanders of DoD Installations report through their chains of command the review results to the DoD Executive Agent so that plans and requirements can be fully coordinated and supported across the Department.

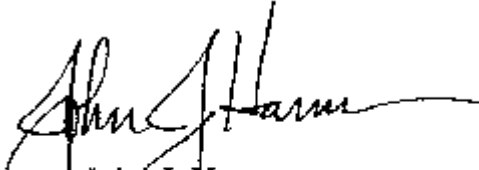


## 6. INFORMATION REQUIREMENTS

The collection of installations and facilities data identified in paragraph 5.2.4., above, is assigned Report Control Symbol DD-A&T(A)760, and the collection of Critical Asset data identified in paragraphs 5.5.1. and 5.7.1., above, is assigned Report Control Symbol DD-POL(A)1747, in accordance with DoD 8910-M (reference (m)). The information collections in paragraphs 5.3.3.1., 5.3.4., and 5.7.6., above, are exempt from licensing in accordance with reference (m).

## 7. EFFECTIVE DATE

This Directive is effective immediately.



John J. Hamre  
Deputy Secretary of Defense

Enclosures - 2

1. References
2. Definitions

E1. ENCLOSURE 1

ENCLOSURE 1  
REFERENCES, continued

- (e) DoD 5025.1-M, "DoD Directives System Procedures," August 1994, authorized by DoD Directive 5025.1, June 24, 1994
- (f) DoD Directive 3025.1, "Military Support to Civil Authorities (SCA)," January 15, 1993
- (g) DoD Directive 3025.12, "Military Assistance for Civil Disturbances," February 4, 1994
- (h) DoD Directive 3025.15, "Military Assistance to Civil Authorities," February 18, 1997
- (i) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988
- (j) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982, authorized by DoD Directive 5240.1, April 25, 1988.
- (k) Title 48, Code of Federal Regulations, "Federal Acquisition Regulations System," October 1, 1996
- (l) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I))," February 12, 1992
- (m) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," November 28, 1986, authorized by DoD Directive 8910.1, June 11, 1993
- (n) DoD Directive 5200.8, "Security of DoD Installations and Resources," April 25, 1991

## E2. ENCLOSURE 2

### DEFINITIONS

E2.1.1. Assurance. In the context of CAAP, assurance is a process of identifying assets deemed critical to the Department of Defense in peacetime, crisis and war; assessing the potential threats to these assets and the capabilities they provide; quantifying the likely non-availability to the Department of Defense under various hazard scenarios; identifying potential actions that can be taken to restore those assets (or functionality they provide) if they are lost, damaged, corrupted, or compromised; and identifying and recommending options to protect, mitigate, and improve the availability of these Critical Assets to the DoD organizations that own, use, and control them. It includes a range of activities to systematically inform planners and decisionmakers of the probability of availability and quality (e.g., integrity, reliability, confidentiality, survivability, endurability, capacity, adequacy) of specific assets or services under given scenarios; quantifying the likely impact of non-availability to the military operation or defense activity; and identifying and prioritizing options to improve the likelihood of the availability of specific assets or services in specific scenarios. Examples of assurance activities that can improve the likelihood of asset availability include protection (preventing, by whatever means, the disruption or corruption of an asset); mitigation or moderation of the effects of disruption or corruption (by controlling the damage, providing alternative services, and reducing demand on the asset); and planning for and providing timely restoral or recovery. Alternatively, plans can be made to absorb the loss of otherwise anticipated services. Assurance of a Critical Asset is the responsibility of the owning or controlling DoD Component.

E2.1.2. Computer Emergency Response Team (CERT). An organization chartered by an information system owner to coordinate and/or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems.

E2.1.3. Critical Asset. Any facility, equipment, service or resource considered essential to DoD operations in peace, crisis and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration. Critical Assets may be DoD assets or other government or private assets, (e.g., Industrial or Infrastructure Critical Assets), domestic or foreign, whose disruption or loss would render DoD Critical Assets ineffective or otherwise seriously disrupt DoD operations. Critical Assets include

both traditional "physical" facilities or equipment, non-physical assets (such as software systems) or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks).

E2.1.4. DoD Executive Agent. The individual designated by position to have and to exercise the assigned responsibility and delegated authority of the Secretary of Defense, as specified in this Directive.

E2.1.5. DoD Infrastructure. Infrastructure owned, operated or provided by the Department of Defense. DoD Infrastructures include the DII, C4ISR, Space, Financial Services, Logistics, Public Works (includes DoD-owned or -operated utilities, roads, rails and railheads and their interface to commercial and other Government Systems), Personnel, Health Affairs and Emergency Preparedness. See also definitions of Infrastructure and National Infrastructure, below.

E2.1.6. DoD Installation. A facility subject to the custody, jurisdiction, or administration of any DoD Component. This term includes, but is not limited to, military reservations, installations, bases, posts, camps, stations, arsenals, or laboratories where a DoD Component has operational responsibility for facility security and defense. Examples are facilities where orders or regulations for protection and security have been issued by the military commander or other specified DoD official under provisions of DoD Directive 5200.8 (reference (n)). Both industrial assets and infrastructure assets, not owned by the Department of Defense, may exist within the boundaries of a military installation.

E2.1.7. Industrial Asset. Any factory, plant, building or structure used for manufacturing, producing, processing, repairing, assembling, storing, or distributing a product or components that supports a DoD Component. A Critical Industrial Asset is an industrial asset deemed essential to DoD operations or the functioning of a Critical Asset

E2.1.8. Information Assurance. Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (See DoD Directive S-3600.1, reference (c).)

E2.1.9. Information System. The entire infrastructure, organization, personnel and components that collect, process, store, transmit, display, disseminate and act on information under reference (c).

E2.1.10. Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, or society as a whole.

E2.1.11. Infrastructure Asset. Any Infrastructure facility, equipment, service or resource that supports a DoD Component. A Critical Infrastructure Asset is an infrastructure asset deemed essential to DoD operations or the functioning of a Critical Asset.

E2.1.12. National Infrastructure. Those infrastructures essential to the functioning of the nation and whose incapacity or destruction would have a debilitating regional or national impact. National infrastructures include telecommunications, electrical power systems, gas and oil transportation and storage, water supply systems, banking and finance, transportation, emergency services, and continuity of government operations.

E2.1.13. Technical Attack. An attack that can be perpetrated by circumventing or nullifying hardware or software protection mechanisms, or exploiting hardware or software vulnerabilities, rather than physical destruction or by subverting system personnel or other users.