Department of Defense

INSTRUCTION

NUMBER 3020.45
April 21, 2008

USD(P)

SUBJECT: Defense Critical Infrastructure Program (DCIP) Management

References: (a) DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005
(b) Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003[1]
(c) National Infrastructure Protection Plan (NIPP), Department of Homeland Security, 2006[2]
(d) Assistant Secretary of Defense (Homeland Defense) Memorandum, "Defense Critical Infrastructure Program (DCIP) Interim Implementation Guidance," July 13, 2006 (hereby canceled)
(e) through (q), see Enclosure l

1. PURPOSE

This Instruction:

1.1. Implements and establishes policy in support of the requirements of Reference (a) to manage the identification, prioritization, and assessment of defense critical infrastructure (DCI) as a comprehensive program. This program shall include the development of adaptive plans and procedures to mitigate risk, restore capability in the event of loss or degradation, support incident management, and protect DCI-related sensitive information.

1.2. Assigns responsibilities governing risk management including the acceptance, remediation, and/or mitigation of DCI risks.

1.3. Assigns responsibilities and prescribes procedures for the implementation of the DCIP.

1.4. Implements policies set forth in References (a) and (b) for the protection of Federal agency and defense industrial base (DIB) critical infrastructure. Supports the unifying structure, identified in Reference (c), for the integration of critical infrastructure protection.

[1] Copies of this document may be found at http://www.dhs.gov/xabout/laws/editorial_0607.shtm.
[2] Copies of this document may be found at http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

1.5. Clarifies the complementary relationships between DCIP and other DoD programs and efforts such as: force protection; antiterrorism; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness.

1.6. Cancels ASD(HD) Memorandum (Reference (d)).

2. APPLICABILITY

This Instruction applies to:

2.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. Each Defense Infrastructure Sector Lead Agent (DISLA) identified in Reference (a).

3. DEFINITIONS

Terms used in this Instruction are defined in Reference (a) and Enclosure 2.

4. POLICY

It is DoD policy that:

4.1. A comprehensive program be implemented that provides centralized program management of common requirements (e.g., program guidance, planning, and oversight) and capabilities (e.g., standardized analytic methods and tools, geospatially referenced infrastructure data, and visualization technology), and oversees decentralized execution of DCIP throughout the Department of Defense. DCIP data about DCI risks shall be available to authorized officials responsible for complementary programs and efforts (identified in Reference (a)) for execution year resolution and for use within out-of-cycle and routine planning, programming, budgeting, and execution (PPBE) submissions to improve overall DoD mission assurance.

4.2. Risk shall be determined through a risk assessment.

4.3. A critical infrastructure program be implemented that supports risk management decisions by responsible authorities to enable the continued execution of DoD mission-essential functions (MEFs) and primary mission essential functions (PMEFs) in support of national essential functions (NEFs) under all circumstances. (See DoD Directive (DoDD) 5100.1,

National Security Presidential Directive 51/Homeland Security Presidential Directive 20, and DoDD 3020.26 (References (e) through (g), respectively).)

4.4. Situational awareness of the risk to DCI shall be maintained.

4.5. Appropriate DCIP information shall be provided to incident management officials responding to incidents (e.g., natural disasters or attacks) to ensure availability of DCI.

4.6. Collaboration shall be fostered among the DoD Components, the DISLAs, other government agencies, and non-governmental DCI owners and operators.

4.7. Maximum use of existing information systems, data sharing technology, information assurance capabilities, and the Global Information Grid in accordance with DoDDs 8000.01, 8100.01, 8320.02, and 8500.01E (References (h) through (k)) shall be leveraged in implementation of DCIP. It is recognized that risk management activities (threat awareness, vulnerability management, and mitigations) of DCIP as it relates to information, information technology, and national security systems is governed by DoD 5200.1-R (Reference (l)), Reference (k), and associated implementing instructions.

4.8. Maximum use, as permissible and appropriate, of existing DoD and non-DoD management structures and processes shall be leveraged to ensure effective and efficient program execution.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA)), under the Under Secretary of Defense for Policy (USD(P)), shall:

5.1.1. Provide policy and guidance for the DCIP and oversee (including but not limited to) the implementation of:

5.1.1.1. DoD Component and DISLA responsibilities.

5.1.1.2. A DCIP program plan.

5.1.1.3. DCI identification across all the DoD Components and defense infrastructure sectors using a mission-focused process that includes all DoD functions as described in Reference (e).

5.1.1.4. DCI vulnerability assessments conducted in accordance with established DCIP standards and benchmarks.

5.1.1.5. Risk assessment.

5.1.1.6. Actions for the remediation and mitigation of risk to DCI, to include monitoring decisions to accept risk to DCI.

5.1.1.7. Incident-response planning to establish and communicate standard program-wide immediate action procedures that DCIP stakeholders may expect to use during emergencies.

5.1.1.8. Education, training, and awareness goals and objectives.

5.1.2. Support the Secretary of Defense's role as the lead sector-specific Federal agency official for DIB critical infrastructure consistent with References (b) and (c).

5.1.3. Develop and issue, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO); and the Chairman of the Joint Chiefs of Staff, a strategy to attain a resilient DCI.

5.1.4. Issue a list of defense critical assets (DCAs) related to NEFs, MEFs, and PMEFs, as defined in References (f) and (g), the DCIP Security Classification Guide (Reference (m)), and the National Defense Strategy (Reference (n)) based upon nominations from the Chairman of the Joint Chiefs of Staff.

5.1.5. Participate in the PPBE process under DoDD 7045.14 (Reference (o)).

5.1.5.1. Advise the Secretary of Defense, the Deputy Secretary of Defense, and USD(P) on major resource allocation and investments, including recommending whether to initiate, continue, modify, or terminate individual DCIP investments.

5.1.5.2. Review DCIP and related DoD program funding requirements and recommend appropriate changes and/or allocations.

5.1.5.3. In coordination with the Chairman of the Joint Chiefs of Staff, compile and assess DoD Component and DISLA DCIP requirements to support resource allocation.

5.1.6. Direct the DCI owner to conduct a DCIP risk assessment within 90 days of the completion of the threat and hazard and vulnerability assessments.

5.1.7. Provide the USD(AT&L) with recommended changes to the Federal Acquisition Regulation, the Defense Federal Acquisition Regulation Supplement, and other procurement regulations as appropriate to implement DCIP.

5.1.8. Provide the Under Secretary of Defense for Intelligence (USD(I)) requirements for intelligence collection, threat assessments, and dissemination of warnings regarding DCI.

5.1.9. Coordinate procedures for appropriate DCI information production and information sharing, consistent with law and Federal requirements, to include taking into account

the safeguards established by the Protected Critical Infrastructure Information (PCII) Program (see part 29 of title 6, Code of Federal Regulations (Reference (p))) and DoD guidance.

5.1.10. Issue a security classification guide consistent with Reference (l) that includes foreign disclosure guidance for data produced by the DCIP.

5.1.11. Establish systems architecture requirements for DCIP consistent with References (i) and (j). (References (i) and (j) describe operational, system, and technical architectural views.)

5.1.12. Establish, maintain, participate in, or lead DCIP forums to:

5.1.12.1. Solicit advice regarding DCIP goals and objectives, direction, requirements, and integration with other management programs.

5.1.12.2. Facilitate collaboration among DCIP participants, other government agencies, non-government agencies, and the private sector consistent with program management, agreements with other Federal agencies, and regulatory requirements.

5.1.13. In coordination with the Under Secretary of Defense for Personnel and Readiness, establish procedures for maintaining task critical asset (TCA) readiness data in the Defense Readiness Reporting System.

5.2. The Heads of the OSD Components, consistent with their respective areas of responsibility (AORs) assigned by Reference (a), shall oversee the DISLA DCIP activities and conduct periodic program reviews to:

5.2.1. Monitor and assist the DISLA to plan and coordinate with the DoD Components to characterize the respective defense infrastructure sectors and identify and prioritize sector-related TCAs.

5.2.2. Ensure that sector TCA data is accessible in conformance with architectural views that address DCIP requirements, Reference (j), and DCIP classification requirements.

5.2.3. Assess progress in executing the Defense Infrastructure Sector Assurance Plan (DISAP) and sector risk management activities.

5.3. The USD(AT&L), in addition to the responsibilities in paragraph 5.2., shall:

5.3.1. Incorporate DCIP requirements into DoD contracting regulations.

5.3.2. Recommend potential solutions to reduce risks to DCI.

5.4. The USD(I), in addition to the responsibilities in paragraph 5.2., shall:

5.4.1. Consistent with U.S. laws and DoD issuances and within the legal authority granted to the Department of Defense and subject to limitations on gathering information on U.S. persons, direct DoD intelligence, counterintelligence, and security activities to:

5.4.1.1. Identify the capability and intent of specific threats to cause loss or damage to DCI and assess the likelihood that such threats will be carried out.

5.4.1.2. Identify the capability and intent of specific intelligence-collection threats to DCI.

5.4.1.3. Coordinate with other appropriate Federal agencies such as the Department of Homeland Security and Federal Bureau of Investigation to obtain threat and hazard information on DoD and DIB critical assets.

5.4.1.4. Produce, triennially or more frequently if required, a multidisciplinary baseline threat assessment addressing the foreign intelligence and security services, terrorism, information operations, sabotage, and proliferation threats related to DCIP.

5.4.1.5. Make intelligence-based indications and warning information related to DCI available to DoD Components and DISLAs.

5.4.1.6. Communicate to DoD Components and DISLAs credible and actionable data concerning threats to DCI.

5.4.1.7. Inform the ASD(HD&ASA), the DoD Components, and DISLAs DCIP Office of Primary Responsibility (OPR) of DCI threat assessment results and changes in the threat.

5.4.1.8. Identify counterintelligence and security measures to mitigate risks and protect DCI.

5.4.2. Establish intelligence collection and counterintelligence policy and priorities to support DCIP activities.

5.5. The ASD(NII)/DoD CIO, in addition to the responsibilities in paragraph 5.2., shall:

5.5.1. Evaluate and incorporate DCIP requirements identified by ASD(HD&ASA), as appropriate, into DoD information assurance policy and guidance.

5.5.2. Identify potential solutions to reduce risk to information, information technology, and national security system components of DCI.

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

5.6.1. Provide timely advice to the ASD(HD&ASA) on changes to Combatant Command DCIP resource requirements in accordance with Reference (o).

5.6.2. Provide to the ASD(HD&ASA), DoD Components, and DISLAs:

5.6.2.1. A list of recommended DCAs, submitted annually and when changes occur, based on the TCA lists provided by the Combatant Commands, Defense Agencies, Military Departments, and the DISLAs.

5.6.2.2. Military operational requirements and risk response priorities for DoD-owned DCI and of non-DoD-owned DCI within the respective AORs of the Combatant Commanders submitted annually and when changes occur.

5.6.3. Establish and execute a DCIP vulnerability assessment program for and in concert with ASD(HD&ASA), and serve as the focal point for consolidating assessment data. The scope of the DCIP vulnerability assessment program will include but is not limited to:

5.6.3.1. Providing annually to the ASD(HD&ASA) a consolidated DCIP vulnerability assessment schedule that is coordinated through the Combatant Commands, Military Departments, Defense Agencies, and DISLAs.

5.6.3.2. Compiling DIB assessment schedules, vulnerability data, and risk response priorities provided by DIB DISLA and forwarding annually to ASD(HD&ASA). Make this schedule available to other DoD Components as necessary.

5.6.3.3. Managing the overall assessment of DCAs. All DCAs must be assessed by a Military Department or Joint Staff-level team at least once every 3 years.

5.6.3.4. Ensuring that all organizations conducting DCIP vulnerability assessments provide subject matter experts as team members and require the use of DCIP standards and benchmarks.

5.6.3.5. Ensuring assessments capture ASD(HD&ASA) baseline elements of information (BEIs), vulnerabilities, and recommended corrective actions. Ensure reports are disseminated to all appropriate DoD Components and DISLAs with a valid interest in the asset.

5.6.3.6. Providing the ASD(HD&ASA) with an annual report on the execution and effectiveness of the DCIP vulnerability assessment program of DCI, including future year resource requirements for the assessment program.

5.6.3.7. Issuing statements of work, formal agreements, or contracts as required to obtain sponsored assessment capability.

5.6.4. Coordinate with the appropriate DoD Components and DISLAs to provide to the ASD(HD&ASA) a consolidated and prioritized set of recommendations regarding actions to remediate or mitigate DCI vulnerabilities and related risks as well as the status of mitigation plans for DCI within the AOR of each command.

5.6.5. Provide to the ASD(HD&ASA), as requested, a report on the status of Office of the Chairman of the Joint Chiefs of Staff and Combatant Command DCIP activities consistent with Reference (a) and this Instruction.

5.7. The Commanders of Combatant Commands shall, within their respective AOR:

5.7.1. Submit to the Chairman of the Joint Chiefs of Staff DCIP OPR changes to command DCIP requirements, including command priorities for DCIP vulnerability assessments and risk response of DCI-related risks.

5.7.2. Conduct analyses of command missions and mission essential tasks (METs) with their associated conditions and standards, and provide results to appropriate DoD Component and DISLA DCIP OPRs to support TCA identification in accordance with the DCIP critical asset identification process.

5.7.2.1. Make command METs and other required tasks or capabilities available in accordance with architectural views that address DCIP requirements and Reference (j) and DCIP security classification requirements.

5.7.2.2. Coordinate and assist with additional DoD Component and DISLA analyses of command missions and related capabilities to identify TCAs necessary to execute these missions.

5.7.2.3. Validate TCAs submitted by the DoD Components as critical to the fulfillment of their assigned missions and submit a compiled, validated list of TCAs to the Chairman of the Joint Chiefs of Staff annually and when changes occur.

5.7.3. Collect and disseminate DCIP-related threats assessments and warnings, as appropriate, to subordinate elements, other DoD Components and DISLAs, and other authorized activities.

5.7.4. Develop and exercise DCI mitigation plans to demonstrate that continuity of operations can be maintained.

5.7.5. Program resources to implement DCIP responsibilities.

5.7.6. Provide, as requested, a report through appropriate reporting channels to the OASD(HD&ASA) on organizational DCIP status and progress, consistent with Reference (a) and this Instruction.

5.8. The Secretaries of the Military Departments; Commander, U.S. 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, having control of DCI assets within their respective AORs, shall:

5.8.1. Identify an OPR to establish, provide resources for, and execute a component program for matters pertaining to the identification, prioritization, assessment, mitigation, remediation, and management of risk to DCI, along with annual DCIP training and exercise resource requirements. Military Departments shall fund and resource, as part of their DCIP requirements submitted in the PPBE process, the establishment and maintenance of an organizational structure to support execution of the DCIP.

5.8.2. Identify, validate, and prioritize DCIP resource requirements and provide adequate resources for DCIP in DoD Components' baseline budgets generated through the PPBE process.

5.8.3. Undertake the following activities in the DoD Component roles as both mission and DCI asset owners:

5.8.3.1. Identify TCAs in support of assigned missions, METs, and/or core functions and provide analysis results to the Chairman of the Joint Chiefs of Staff DCIP OPR. Coordinate with other DoD Components and DISLAs as necessary to determine scope and parameters of their missions, METs, and core functions assigned to the organization for execution to identify TCAs.

5.8.3.2. For DCI, provide and maintain DoD Component BEI data on this asset and make this data accessible in accordance with architectural views that address DCIP requirements, Reference (j), and DCIP security classification requirements.

5.8.3.3. For DCAs, appoint in writing a DCIP point of contact (POC) for that asset.

5.8.3.4. Provide DCI-specific threat and hazard information to appropriate DoD Components and DISLAs to establish an enhanced specific threat and hazard profile. Provide update whenever changes occur to threats, hazards, or vulnerabilities or in response to an incident. Notify law enforcement or counterintelligence authorities, as appropriate.

5.8.3.5. Schedule and conduct vulnerability and risk assessments for DCI owned by the DoD Component in accordance with DCIP standards and benchmarks. Coordinate with the Chairman of the Joint Chiefs of Staff on vulnerability assessments scheduled by the DoD Component, or referred to the Chairman of the Joint Chiefs of Staff assessment program for execution. Provide risk and vulnerability assessment results to the appropriate DoD Components and DISLAs.

5.8.3.6. Develop, coordinate, and record courses of action (COAs) for and provide to appropriate DoD Components and DISLAs the status and progress of risk response and/or acceptance of risk to DCI assets controlled by the DoD Component.

5.8.4. Provide, as requested, a report through appropriate reporting channels to the OASD(HD&ASA) on organizational DCIP status and progress, consistent with Reference (a) and this Instruction.

5.8.5. Prepare and coordinate risk assessment options and recommendations for controlled DCI in accordance with Enclosure 3.

5.8.6. Provide DCIP information during defense support to civil authorities or consequence management operations and exercises to OASD(HD&ASA), appropriate DoD Components, and DISLAs.

5.8.7. Implement training and education activities designed to meet DCIP education and training goals and objectives.

5.8.8. Provide resources and support to the DISLAs to accomplish the actions of the various defense infrastructure sector working groups and to develop and maintain the DISAP.

5.9. The Defense Infrastructure Sector Lead Agents as assigned in DoD Directive 3020.40 shall:

5.9.1. Charter a Defense Infrastructure Sector Working Group of applicable DoD Component DCIP sector functional representatives to develop and coordinate sector plans and activities.

5.9.2. Serve as the non-DoD asset owners' representative for DCI issues in their designated AORs. Where appropriate, establish relationships with the asset owners.

5.9.3. Identify sector-related TCAs and inter- and intra-dependencies for sector functions and in support of mission and asset owners' analyses and submit a compiled, validated list of TCAs related to sector functions to the Office of the Chairman of the Joint Chiefs of Staff annually and when changes occur.

5.9.4. Maintain a defense infrastructure sector characterization; make the data accessible in accordance with Reference (j) and DCIP security classification requirements; and provide data on an incident's sector-related effect on the health of the sector to appropriate authorities.

5.9.5. Provide an annual summary on the current status and changes to health of the sector and recommendations on remediation and mitigation of defense infrastructure sector-related risks to the ASD(HD&ASA), the Chairman of the Joint Chiefs of Staff, DoD Component that owns the asset, and PSA responsible for the defense infrastructure sector.

5.9.6. Develop and maintain a DISAP (Enclosure 4) that includes DCIP risk management considerations.

5.9.7. Maintain awareness of sector DCI remediation and mitigation alternatives and plans, and provide assistance to asset owners in developing those plans, as requested.

5.9.8. Provide, as requested, a report through appropriate reporting channels to the OASD(HD&ASA) on organizational DCIP status and progress, consistent with Reference (a) and this Instruction.

6. PROCEDURES

6.1. The DCIP supports a risk management process that seeks to ensure DCI availability with a priority focus on DCAs. For this particular program, the risk management process is comprised of a risk assessment component that identifies critical assets and infrastructure interdependencies that support DoD missions. Applicable follow-on threat and vulnerability assessments are then conducted on those assets to complete the risk assessment. Properly implemented risk assessment procedures of critical assets enable informed risk management decisions, leading to an appropriate risk response. The risk response component ensures that limited resources are optimally allocated toward those assets deemed most important to overall mission success for the Department of Defense, and for which it has been determined that the identified level of risk is unacceptable. These actions comprise the major elements of DCIP risk management.

6.2. Detailed program procedures are outlined in Enclosure 3.

7. INFORMATION AND DATA REQUIREMENTS

7.1. The vulnerability assessment reporting requirements in this Instruction have been assigned Report Control Symbol (RCS) DD-POL(AR) 2294 in accordance with DoD 8910.1-M (Reference (q)).

7.2. The risk assessments are exempt from licensing in accordance with paragraph C4.4.2. of Reference (q).

7.3. Architectural views that address DCIP data requirements will:

7.3.1. Catalog the DCIP BEIs.

7.3.2. Include the information sharing requirements and methodology needed to support the DCIP.

8. RELEASABILITY

UNLIMITED. This Instruction is approved for public release. Copies may be obtained through the internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

9. EFFECTIVE DATE

This Instruction is effective immediately.

Ryan Henry
Principal Deputy Under Secretary of Defense
for Policy

Enclosures – 5

E1. References, continued
E2. Definitions
E3. DCIP Process and Procedures
E4. DISAP
E5. Acronyms

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Directive 5100.1, "Functions of the Department of Defense and Its Major Components," August 1, 2002
(f) National Security Presidential Directive 51/Homeland Security Presidential Directive 20, "National Continuity Policy", May 2007[3]
(g) DoD Directive 3020.26, "Defense Continuity Program (DCP)," September 8, 2004
(h) DoD Directive 8000.01, "Management of DoD Information Resources and Information Technology," February 27, 2002
(i) DoD Directive 8100.01, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(j) DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004
(k) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(l) DoD 5200.1-R, "Information Security Program," January 14, 1997
(m) Defense Critical Infrastructure Program (DCIP) Security Classification Guide, May 2007
(n) National Defense Strategy, March 2005[4]
(o) DoD Directive 7045.14, "The Planning, Programming, and Budgeting System (PPBS)," May 22, 1984
(p) Part 29 of title 6, Code of Federal Regulations
(q) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998

[3] Copies of this document may be found at http://www.dhs.gov/xabout/laws/editorial_0607.shtm.
[4] Copies of this document may be found at http://www.defenselink.mil/news/Mar2005/d20050318nds1.pdf

E2. ENCLOSURE 2

DEFINITIONS

E2.1. Asset Owner. The DoD Components with responsibility for a DoD asset, or organizations that own or operate a non-DoD asset.

E2.2. Baseline Elements of Information. The minimum defined information requirements necessary to support a risk management decision.

E2.3. Benchmarks. For the purpose of this Instruction, a series of necessary objectives-based questions for the Defense Critical Infrastructure Program the answers to which indicate the degree to which specific standards have been met.

E2.4. Criticality. For the purpose of this Instruction, a metric used to describe the consequence of loss of an asset, based on the effect the incapacitation or destruction of the asset would have on DoD operations and the ability of the Department of Defense to fulfill its missions.

E2.5. Mission Owner. DoD organizations having responsibility for the execution of missions assigned by statute or the Secretary of Defense, and supporting organizations with responsibility for execution of all or part of those missions.

E2.6. Reconstitution. The process of restoring critical assets and their necessary infrastructure support systems (or their functionality) to pre-incident operational status.

E2.7. Resiliency. The characteristic or capability to maintain functionality and structure (or degrade gracefully) in the face of internal and external change.

E2.8. Susceptibility. The inherent capacity of an asset to be affected by one or more threats or hazards.

E2.9. Task Asset. An asset that is directly used to support execution of one or more operations, tasks, activities, or mission essential tasks (METs).

E2.10. Task Critical Asset (TCA). 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 Components or Defense Infrastructure Sector Lead Agents to execute the task or MET it supports. TCAs are used to identify defense critical assets.

E3. ENCLOSURE 3

DCIP PROCESS AND PROCEDURES

E3.1. PROGRAM MANAGEMENT

E3.1.1. Appropriate DoD Components and DISLA DCIP support:

E3.1.1.1. Sector characterization.

E3.1.1.2. Identification and prioritization of DCI in accordance with approved guidance.

E3.1.1.3. DCIP threat and hazard identification.

E3.1.1.4. DCIP vulnerability assessment.

E3.1.1.5. Risk assessment.

E3.1.1.6. Risk response including risk acceptance, remediation, mitigation, and reconstitution activities.

E3.1.1.7. DCIP education and outreach.

E3.1.1.8. DCIP training and exercising.

E3.1.2. DoD Components and DISLA DCIP OPRs coordinate data flows between and among DoD Components and DISLAs consistent with section E3. Data flows required to execute DCIP activities within a Component will use established communications channels.

E3.1.3. DoD Components shall designate, train, and provide resources for a full-time staff to execute a component-level program and support subordinate DCIP offices to administer their respective DCI programs. The DISLAs shall designate, train, and provide resources for a full-time staff to execute a sector-level program to administer their respective DCI programs.

E3.1.4. DoD Components that own one or more DCAs must have a DCIP POC appointed in writing.

E3.1.5. Combatant Commands and the Military Departments shall:

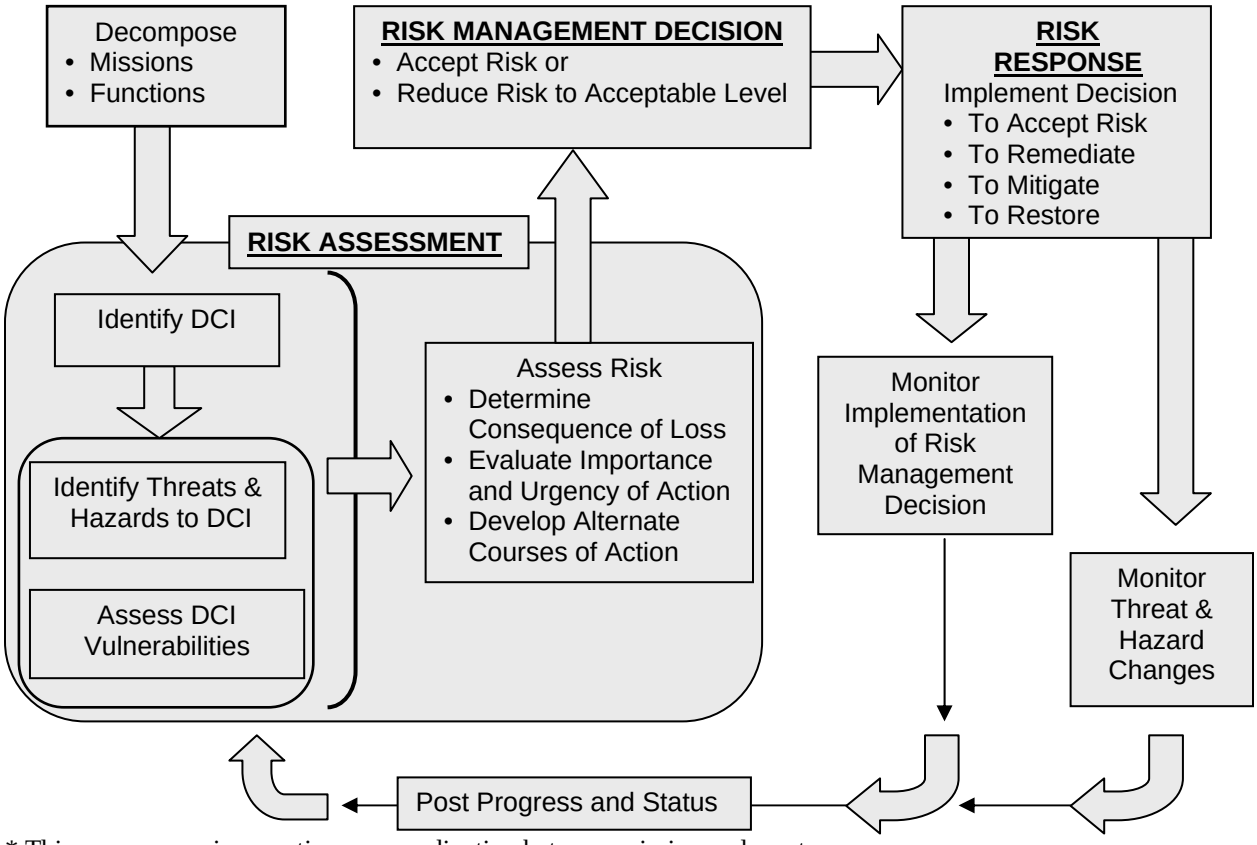
E3.1.5.1. Execute annual exercises, either separately or in conjunction with existing exercises, to integrate other Federal departments and agencies in the risk reduction and in the protection, recovery, and restoration of DCI notionally affected by the full spectrum of threats and hazards. Coordinate, as possible, for maximum mission owner participation to limit redundant effect upon the asset owner.

E3.1.5.2. Direct the incorporation of DCIP plans into joint operations, training, and exercises. Commanders shall ensure the submission of DCIP lessons learned in accordance with the Joint Lessons Learned Program.

E3.2. RISK MANAGEMENT

DCIP is a risk management program that seeks to ensure DCI availability. Risk assessment and risk response are the major elements of DCIP risk management. The component parts of risk assessment and risk response and their relationship to one another are illustrated in Figure E3.F1. and are discussed in the following paragraphs.

Figure E3.F1. DCIP Risk Management Process Model*



* This process requires continuous coordination between mission and asset owners

E3.2.1. Risk Assessment

E3.2.1.1. Core Elements. The core elements of the DCIP risk assessment process are criticality determination, threats and hazards assessment, and vulnerability assessment. For complete and accurate risk assessment, the evaluation of each element must be accomplished (individually and collectively), as well as the assessment of the interactions and interdependencies involved (criticality, threat and/or hazard, vulnerability).

E3.2.1.2. Assessment Timeline. A risk assessment will be conducted within 90 days of the completion of the threat/hazard and vulnerability assessments for a given DCI. Because of the dynamic risk environment, the ASD(HD&ASA) or DoD Component DCI owner may require an earlier or additional DCI risk assessment to determine the need for a PPBE out-of-cycle resource decision.

E3.2.1.3. Assessment Results. DCIP risk assessments will result in sufficient information to support a risk decision to either accept the risk associated with the possible degradation or loss of the DCI or to adopt a COA entailing remediation, mitigation, and/or reconstitution.

E3.2.1.4. Criticality Determination. The Department of Defense identifies DCI using a consistent, repeatable, mission-focused analysis process to identify TCAs and an effects-based analysis to identify DCAs from the list of TCAs.

E3.2.1.4.1. The identification of TCAs is the responsibility of mission owners, asset owners, and DISLAs.

E3.2.1.4.2. The expected results from this criticality process include:

E3.2.1.4.2.1. Identification of TCAs associated with a hierarchy of METs, starting with METs identified by the Combatant Commands or Defense Agencies, by the responsibilities of the Military Departments, or by sector function.

E3.2.1.4.2.2. DCAs, as nominated by the Chairman of the Joint Chiefs of Staff and approved by OASD(HD&ASA).

E3.2.1.4.2.3. TCAs BEI data.

E3.2.1.4.2.4. For DoD information system-related DCI, the Mission Assurance Category of the asset as defined in Reference (j).

E3.2.1.4.3. The procedures for identification of DCI are as follows:

E3.2.1.4.3.1. Combatant Commands and Defense Agencies determine their METs and supporting mission owners link their METs to the Combatant Command and Defense Agency METs. Combatant Commands and Defense Agencies review and validate the combined list of linked METs supporting each of their METs. Military Departments identify their responsibilities. Sectors identify their sector functions.

E3.2.1.4.3.1.1. Based on the list of validated, linked METs, Military Department responsibilities, and sector functions, appropriate mission owners, asset owners, and DISLAs identify the task assets (TAs) required to accomplish each.

E3.2.1.4.3.1.2. Mission owners, in conjunction with asset owners and DISLAs, review each TA to identify and nominate TCAs to their respective Combatant Commanders, Military Departments, Defense Agencies, or DISLA.

E3.2.1.4.3.1.3. Combatant Commanders, Military Departments, Defense Agencies, and DISLAs each validate the submitted TCAs and then submit their final list of TCAs to the Chairman of the Joint Chiefs of Staff DCIP OPR.

E3.2.1.4.3.2. The Chairman of the Joint Chiefs of Staff DCIP OPR will integrate Combatant Command, Military Department, Defense Agency, and DISLA TCA submissions into a DoD-wide TCA list and then nominate a recommended list of DCAs for submission to the ASD(HD&ASA) at least annually.

E3.2.1.4.3.3. The ASD(HD&ASA) will review submitted DCA nominations, approve DCAs, and submit the DCA list to appropriate DoD Components and DISLAs.

E3.2.1.5. Threats and Hazards Assessment. The Department of Defense recognizes the need to establish a consistent, systematic approach to identifying, analyzing, disseminating, and forecasting threats and hazards to DCI in order to assess and respond to DCIP-related risk.

E3.2.1.5.1. The DoD Components and the DIB DISLA with assigned DCIP risk-assessment responsibilities shall require the use of threat and hazard information in assessment of DCI for which they are responsible.

E3.2.1.5.2. The USD(I) or its designated authority will prepare and maintain a multidisciplinary threat baseline. This baseline will include threats related to foreign intelligence and security services, terrorism, information operations, sabotage, and proliferation that could adversely affect DCI.

E3.2.1.5.3. The products of this threat and hazard process include:

E3.2.1.5.3.1. A full-spectrum threat baseline covering known or suspected threat actors and their capabilities and intent.

E3.2.1.5.3.2. An enhanced, DCI-specific threat and hazard profile resulting from DCI owner threat and hazard analysis.

E3.2.1.5.4. The DoD Components and the DISLAs shall establish procedures and channels through which DCI-related threat and hazard information is communicated with subordinate elements, other DoD Components, and other authorized activities in the conduct of DCIP risk assessment and risk response activities.

E3.2.1.5.5. Mission and asset owners shall provide regional or DCI-specific threat and hazard information to appropriate DoD Components and DISLAs through established channels that will result in an enhanced, DCI-specific threat and hazard profile. This information

will be updated whenever a change occurs at a DCI that affects threats, hazards, or vulnerabilities or in response to an incident.

E3.2.1.5.5.1. Asset owners shall validate existing threat and hazard profile data and provide updates, as appropriate, during the conduct of DCIP vulnerability assessments.

E3.2.1.5.5.2. DCI owners will use validated, enhanced threat and hazard profiles in conducting risk assessments.

E3.2.1.6. DCIP Vulnerability Assessment. The ASD(HD&ASA), in coordination with USD(AT&L) and ASD(NII)/DoD CIO, will establish a DCIP vulnerability assessment process that identifies DCI vulnerabilities through the use of approved DCIP vulnerability assessment standards and benchmarks, including system and network vulnerabilities, to ensure consistent and comprehensive assessment practices.

E3.2.1.6.1. The DoD Components and DISLAs will submit annually a prioritized list and recommended timeline for the conduct of DCIP vulnerability assessments to the Chairman of the Joint Chiefs of Staff OPR. The DIB DISLA will likewise submit a prioritized assessment list for DIB DCI.

E3.2.1.6.2. The Chairman of the Joint Chiefs of Staff DCIP OPR, as lead and in coordination with DoD Components and DISLAs, will deconflict DoD Component and DISLA DCIP vulnerability assessment recommendations and submit a consolidated, prioritized list to ASD(HD&ASA) along with a timeline for these assessments. In preparing this list, the Chairman of the Joint Chiefs of Staff DCIP OPR will consider expanding the scope of a DCIP vulnerability assessment for cases in which more than one DCI is located at an installation or site. The consolidated list will include assessments sponsored by DoD Components and the Chairman of the Joint Chiefs of Staff.

E3.2.1.6.3. The Chairman of the Joint Chiefs of Staff DCIP OPR, DCI owners, DIB DISLA, or their representatives will conduct DCIP vulnerability assessments in accordance with the DCIP vulnerability assessment process. A DCIP vulnerability assessment may be a self-assessment or may be either a DoD Component-led or third-party assessment conducted by subject matter experts.

E3.2.1.6.4. A DoD Component-led or third-party DCIP vulnerability assessment will be conducted at least once every 3 years for each DCA in accordance with a mission focus statement that lays out the scope of the assessment and its intended outcomes. Each DCIP vulnerability assessment will result in:

E3.2.1.6.4.1. Analysis of DCA system design, operation, and supporting infrastructure for the purpose of identifying vulnerabilities.

E3.2.1.6.4.2. Assessment of vulnerabilities to damage mechanisms associated with the DCI threat/hazard profile, taking into account factors of susceptibility, accessibility, and existing countermeasures.

E3.2.1.6.4.3. The identified effect of vulnerability exploitation on asset owners and mission owners.

E3.2.1.6.4.4. Recommended COAs where mitigation or remediation is warranted.

E3.2.1.6.4.5. A formal assessment report for DoD owned assets being submitted to the OASD(HD&ASA) and DCIP OPRs of the Chairman of the Joint Chiefs of Staff, mission owner, applicable portfolio managers, and asset owner for both the installation level and Military Department or Defense Agency level that covers the elements listed in subparagraphs E3.2.1.6.4.1. through E3.2.1.6.4.4.

E3.2.1.6.4.6. A formal assessment report for non-DoD owned DIB assets being submitted to the DIB DISLA that covers the elements listed in subparagraphs E3.2.1.6.4.1. through E3.2.1.6.4.4.

E3.2.1.6.5. Each DCIP vulnerability assessment will be conducted in accordance with the DCIP Standards and Benchmarks and a mission focus statement that is produced and executed by the DoD Component serving as the assessment sponsor; the DCI owner or the DIB DISLA, as a representative of a non-DoD DIB asset owner; and the assessment team chief. This statement will specify:

E3.2.1.6.5.1. Mission, MET, sector function and/or DIB business operations, and DCI to be assessed.

E3.2.1.6.5.2. DCI performance standards and conditions necessary for mission success.

E3.2.1.6.5.3. Scope of the assessment in terms of location, focus, and limits on offsite supporting infrastructure analysis.

E3.2.1.6.5.4. Assessment team composition in terms of number of staff and subject matter expertise represented.

E3.2.1.6.5.5. Support to be provided by the assessment sponsor.

E3.2.1.6.5.6. Support to be provided by the DCI owner and supporting installation personnel, including access to staff and materials.

E3.2.1.6.5.7. Designated POCs for the sponsor, asset owner, supporting installation, and assessment team.

E3.2.1.6.5.8. Assessment schedule.

E3.2.1.6.5.9. Assessment products.

E3.2.1.6.5.10. Provisions for changing the scope of the assessment, if warranted.

E3.2.1.7. Assess Risk and Recommend COA(s). A DCIP risk assessment, produced by the DCI owner, develops options and a recommendation on whether and how to reduce risks to a DCI. The information input to this process includes:

E3.2.1.7.1. Criticality process results including:

E3.2.1.7.1.1. Identified DCI.

E3.2.1.7.1.2. TCA BEI data.

E3.2.1.7.1.3. For DoD information system-related DCI, the Mission Assurance Category of the asset as defined in Reference (j).

E3.2.1.7.2. Threat and hazard process results, including:

E3.2.1.7.2.1. Strategic, full-spectrum threat baseline.

E3.2.1.7.2.2. Enhanced, DCI-specific threat and hazard profile.

E3.2.1.7.3. DCIP vulnerability assessment process results, including:

E3.2.1.7.3.1. Vulnerabilities.

E3.2.1.7.3.2. Effect on asset owner.

E3.2.1.7.3.3. Recommended remediation options and resource estimates to repair, engineer, or acquire fixes for specific vulnerabilities.

E3.2.1.7.3.4. Recommended mitigation options to implement operational workarounds.

E3.2.1.7.4. Other information that influences risk reduction decisions that may have not been identified by the processes outlined in subparagraphs E3.2.1.1. through E3.2.1.7. This information includes:

E3.2.1.7.4.1. Established business rules.

E3.2.1.7.4.2. Resource availability to redress vulnerabilities.

E3.2.1.7.4.3. Expected time frame for a replacement capability.

E3.2.1.7.4.4. The importance and urgency for taking action based on an impending threat or hazard, as well as political or other non-technical factors.

E3.2.1.7.4.5. Measures to provide a more resilient DCI.

E3.2.1.7.5. A risk assessment submitted for decision examines the aggregation of the information described in subparagraphs E3.2.1.4.3. through E3.2.1.7.4. and presents a defensible COA from among a reasonable range of alternatives. This means that each COA is supported by:

E3.2.1.7.5.1. Available quantitative and qualitative information from the three risk assessment elements described in subparagraphs E3.2.1.4 through E3.2.1.6.

E3.2.1.7.5.2. Technology- or process-based options for reducing risk.

E3.2.1.7.5.3. The resources and time required to implement the COA.

E3.2.1.7.5.4. The effect on the Department of Defense and national interests if no action is taken.

E3.2.1.7.6. The results of each DCIP risk assessment, including options to reduce risk, shall be provided by the DoD Component who is the DCI owner (or by the DIB DISLA in the case of non-DoD owned DIB DCI) to the appropriate DoD Components and DISLAs. Additionally, officials responsible for conducting the risk assessment will post the risk assessment information consistent with the information security and sharing policy, Reference (i), the DCIP security classification guide, and restrictions on dissemination of PCII (Reference (p)).

E3.2.1.7.7. To ensure current awareness of the effect of a DCI on military operations, the Chairman of the Joint Chiefs of Staff shall inform the DCI owner and the appropriate DISLA of changes to DCI-related military operational requirements or post those changes, if appropriate.

E3.2.2. Risk Management Decision

E3.2.2.1. Upon receipt of risk assessment options, recommendations, and support information for a DCA, OASD(HD&ASA) will coordinate with the Chairman of the Joint Chiefs of Staff, appropriate mission owners, the department- or agency-level asset owner, appropriate DISLAs, the USD(AT&L) and the ASD(NII)/DoD CIO to make a coordinated risk management decision; identify means to fund this decision, including advocacy to be provided; and determine the long-term solution to reducing the criticality of the DCA to the Department of Defense. All DCA risk management decisions, to include risk acceptance, will be coordinated as outlined above and documented.

E3.2.2.1. Upon receipt of risk assessment options, recommendations, and support information for all other DCI, the asset owner will coordinate with the appropriate mission owners and DISLAs to make a coordinated risk management decision and identify means to fund this decision, including advocacy to be provided. All DCI risk management decisions, to include risk acceptance, will be coordinated as outlined above and documented.

E3.2.3. Risk Response

E3.2.3.1. Risk response implements a decision by the DCI owner to expend resources to reduce the DCI risk or restore the degraded or destroyed DCI capability. In the context of the DCIP, risk response consists of processes undertaken by DCI owners, mission owners, and incident management and response personnel to minimize the potential loss of DCI capability or improve the protection of DCI from known threats and hazards. When protection fails, risk response should include plans and actions focused on DCI resiliency. These efforts will be designed to ensure that the DCI is available to provide at least minimum functionality required to support the mission.

E3.2.3.2. The core elements of risk response are remediation, mitigation, and reconstitution.

E3.2.3.2.1. Remediation is the responsibility of the DCI owner. Remediation actions are intended to redress design or operational environment flaws that could have an adverse effect on the availability of the DCI, not actions to improve functionality or structure.

E3.2.3.2.2. Mitigation is the responsibility of the mission owner in support of and in coordination with the Combatant Commander in whose AOR the DCI is located or under whose authority the DCI is placed.

E3.2.3.2.3. Reconstitution is the responsibility of the DCI owner.

E3.2.3.3. DCI owners will:

E3.2.3.3.1. Make a DCIP risk management decision in accordance with paragraph E3.2.2.

E3.2.3.3.2. Make available to affected DoD Components and DISLAs the status of the DCI and the status and progress in implementing the risk decision.

E3.2.3.3.3. Monitor DCI status and progress in implementing the DCIP risk management decision.

E4. ENCLOSURE 4

DISAP

E4.1. REQUIREMENT

Reference (a) requires each DISLA to develop and coordinate a DISAP for their sector. The guidance in this Enclosure prescribes the elements of the plan and the procedures for its development and coordination.

E4.2. ELEMENTS OF THE DISAP

E4.2.1. Executive Summary. Depict, in textual and graphical format, the overall risk posture of the sector. Use this section to describe the overall "health" of the sector. The "health" of the sector identifies whether or not the systems, functions, and assets within the sector will be available and functioning during a time of crisis. From a process standpoint, it is the overall ability of the sector to perform essential functions based on DoD Components' assessed risk and mitigation plans for individual sector critical assets.

E4.2.2. Section 1 – Introduction and Background. Describe the defense infrastructure sector and its scope. Describe the elements of the sector program including, but not limited to: program goals and objectives; program management; how the sector program conforms to the DCIP activities prescribed in this Instruction; and requirements for coordination of sector plans with DoD Components, other DISLAs, and government or private sector organizations, as appropriate.

E4.2.3. Section 2 – [name Sector] Defense Infrastructure Sector. Provide a more detailed description of the sector. Describe other authoritative guidance to which the sector program responds; sector functions; DoD and other government agencies that oversee and/or perform sector functions and participate in DCIP sector activities; and the purpose and relevance of the DCIP sector program to the execution of DoD missions within each Combatant Command AOR.

E4.2.4. Section 3 -- Program Management. Describe the sector program management structure, leadership, and support roles and functions. Provide the resource requirements for the current year through the FYDP. Describe the outcomes to be achieved, including the metrics used to measure accomplishment. Describe the strategy for conducting the sector program and identify sector goals, objectives, and activities in the context of the DCIP and the benchmarks, outcomes, and measures required to achieve those goals and objectives. Summarize how the sector program conforms to the DCIP activities prescribed in this Instruction.

E4.2.5. Section 4 -- Risk Assessment. Describe how the DCIP risk assessment core activities described in this Instruction are performed for the sector. Describe the activity the sector will pursue to perform and maintain a current sector characterization, identify critical assets and intra- and inter-Sector dependencies, and coordinate sector vulnerability assessments

of declared DCI. Describe the policies, decision rules, and procedures used to recommend risk remediation, mitigation, and reconstitution and to whom these recommendations are made.

E4.2.6. Section 5 -- Risk Response. Describe the sector procedures for monitoring the status of sector DCI and for monitoring the progress of DCI and DCI-related remediation, mitigation, and reconstitution activities. Identify the major DoD Component POCs (office symbols and/or operations centers) that provide the SIPRNet and/or NIPRNet URL on which sector status information and sector POC data is maintained.

E4.3. DISAP DEVELOPMENT AND COORDINATION PROCEDURES

Each DISLA will prepare a DISAP and coordinate it with the sector Critical Infrastructure Assurance Officer and DoD Component DCIP OPRs.

E5. ENCLOSURE 5

ACRONYMS AND ABBREVIATIONS

AOR	area of responsibility
ASD(HD&ASA)	Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs)
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration /DoD Chief Information Officer
BEI	baseline element of information
COA	course of action
DCA	defense critical asset
DCI	defense critical infrastructure
DCIP	Defense Critical Infrastructure Program
DIB	defense industrial base
DISAP	Defense Infrastructure Sector Assurance Plan
DISLA	Defense Infrastructure Sector Lead Agent
DoD	Department of Defense
DoDD	Department of Defense Directive
MEF	mission-essential function
MET	mission essential task
NEF	national essential function
OPR	office of primary responsibility
OSD	Office of the Secretary of Defense
PMEF	primary mission essential task
PPBE	Planning, Programming, Budgeting and Execution System
PSA	principal staff assistant
TA	task asset
TCA	task critical asset
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy