



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

OCT 11 2011

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR OF THE DEPARTMENT OF DEFENSE FIELD
ACTIVITIES

SUBJECT: Cross Domain Support Element (CDSE) Responsibilities

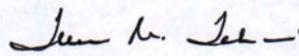
- References: (a) DoD CIO and IC CIO Memorandum, "Establishment of a Department of Defense (DoD)/Intelligence Community (IC) Unified Cross Domain Management Office (CDMO)", July 10, 2006
(b) Unified Cross Domain Management Office (UCDMO) Charter, March 1, 2007
(c) Chairman of the Joint Chiefs of Staff Instruction 6211.02C, "Defense Information System Network (DISN): Policy and Responsibilities," July 9, 2008

Reference (a) established the Unified Cross Domain Management (UCDMO) to more effectively share information across security domains throughout the Federal government using uniform solutions and at less overall cost to the government. Reference (b) specifies the functions, responsibilities and operation of the UCDMO. Reference (c) establishes policies and responsibilities for connection of information systems to the Defense Information System Network, including those employing cross domain solutions (CDS).

In accordance with Reference (c), each DoD Component with an existing or planned CDS is already required to have designated an office to coordinate cross domain activities with the UCDMO. The offices should have reporting responsibilities to their respective Chief Information Officers and Authorizing Officials in order to ensure the support they provide is consistent with other applicable DoD and Component level information assurance and risk management policies. They must also be prepared to transition to Cross Domain Support Elements (CDSEs) under a new DoD instruction, to be developed and coordinated within the next year, on how CDSs are to be implemented, operated, and managed within the DoD.

Under the new instruction, each Component will be responsible for establishing a CDSE or entering into an agreement with another Component's CDSE. Attachment 1 delineates the responsibilities a CDSE will be expected to fulfill under the new DoD instruction. Many have already been implemented by the DoD Components in accordance with Reference (c), but it is recognized that the DoD Components are at different levels of maturity in implementation. The DoD Components should take action to allocate resources and fully develop the necessary technical knowledge to perform the duties described in Attachment 1 in order to effect a timely and smooth transition to CDSEs under the new instruction.

The point of contact for this matter is Mr. Frank Sinkular, Acting Director, UCDDMO at email: fjsinku@nsa.gov, (240) 373-0796.



Teresa M. Takai

Attachment:
As stated

ATTACHMENT 1

CROSS DOMAIN SUPPORT ELEMENT (CDSE) RESPONSIBILITIES

- 1) Be the focal point for and manage all cross domain related activities in their respective DoD Components to include but not limited to keeping the UCDMO informed of new requirements, customer needs, and capability gaps.
- 2) Maintain proficiency in the cross domain capabilities provided by Enterprise Services (ES) and the UCDMO baseline solutions.
- 3) Use ES as the preferred method of addressing cross domain requirements. As mission dictates, select baseline solutions when an ES is not appropriate.
- 4) Ensure that any new cross domain technology developments:
 - Are fully coordinated with the UCDMO;
 - Are in line with the goals and objectives of the Cross Domain Community Roadmap and;
 - Fill identified capability gaps.
- 5) Coordinate and support the DoD Component's cross domain related certification and accreditation activities.
- 6) Coordinate the review, validation, and prioritization of cross domain requirements throughout the implementing DoD Component's acquisition and SDLC¹.
- 7) Ensure that information assurance requirements for cross domain related activities are properly addressed throughout the SDLC.
- 8) Maintain cognizance of Component cross domain related expenditures to include research, development, implementation, and operations.
- 9) Actively participate in applicable cross domain community forums [e.g. Cross Domain Resolution Board (CDRB), Community Security Test Group (CSTG), Requirements Security Engineering Group (RSEG), tiger teams, working groups, etc.] to represent its organizational cross domain needs.
- 10) Maintain access to information regarding cross domain requirements, technology developments, implementations, installations, and configurations (to include updates and patches) within the supported DoD Component's jurisdiction for periodic reporting to the UCDMO via the SIPRNet GIG Interconnection Approval Process (GIAP) System (SGS). Update and revalidate at the end of each calendar year or anytime the data changes.

¹ SDLC includes the initial concept, requirements, design, development, testing and evaluation, operations and maintenance, and disposal or sunset phases