



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY 16 2007

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION,
TECHNOLOGY AND LOGISTICS

SUBJECT: Response to Program Decision Memorandum III (PDM III)

The Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Installation Protection Program Action Plan, submitted in response to a requirement of the PDM III resulting from the Quadrennial Defense Review, is approved for execution. Please provide an update to this office in 180 days on the status of implementation.

A handwritten signature in black ink, appearing to read "Andrew England".

cc:

Secretaries of the Military Departments
Under Secretary of Defense for Policy
Under Secretary of Defense (Comptroller)
Under Secretary of Defense for Personnel and Readiness
Under Secretary of Defense for Intelligence



**CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND HIGH-
YIELD EXPLOSIVES (CBRNE) INSTALLATION PROTECTION (IP)
ACTION PLAN
May 2007
OUSD(AT&L)**

Purpose. This plan provides a coordinated path forward for an improved CBRNE IP strategy based on key recommendations from the June 2006 CBRNE IP Study Report (the “Study”). This effort will be lead by a single steering committee, responsible for coordinating development of clear policy and guidance, effective standards, and both non-material and material capability solutions. This plan describes the implementation, strategy, tasks and schedule required to improve protection of DoD installations against CBRNE threats. The overall goal is to improve installation protection by resolving long-standing policy and guidance gaps. Key objectives include transitioning DoD CBRNE-IP to a standards-based approach built on clear policies and capability definitions and incorporating CBRNE IP into an all-hazards emergency preparedness framework.

Background. In 2005, Program Decision Memorandum (PDM) III (Combating WMD, 21 Dec 2005) tasked the Under Secretary of Defense (Acquisitions, Technology and Logistics) (USD(AT&L)), in coordination with the Chairman of the Joint Chiefs of Staff (CJCS), to develop and submit a revised plan for CBRNE Installation Protection to the Deputy Secretary of Defense (DepSecDef). The work to fulfill PDM requirements began with a thorough study of the CBRNE Installation Protection program which provided recommendations to improve CBRNE IP. This action plan, based on the Study, fulfills the PDM III requirement to develop a revised plan for CBRNE IP.

DoD installation protection efforts, based primarily on DoD Antiterrorism directives and instructions, (DoD Directive 2000.12, DoD Instruction (DoDI) 2000.16, and DoDI 2000.18), have evolved over the past decade. Late in 2002 the Department allocated over one billion dollars (PDM I, Dec 2002) to procure chemical and biological protection for 200 installations (185 CONUS, 15 OCONUS) through the newly created Guardian Installation Protection Program (IPP), managed by Joint Program Manager Guardian (JPMG). In addition to chemical and biological protection, the program included nuclear/radiological equipment and prescribed that enhancements be integrated with ongoing efforts to protect installations against attacks with high-yield explosives.

PDM III reduced procurement funding for the IPP by \$535M and directed USD(AT&L), in coordination with the CJCS, to develop and submit a revised plan for enhancing CBRNE IP. The Study was sponsored by the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs (ATSD(NCB)) and the Joint Requirements Office for CBRN Defense (JRO-CBRND).

The CBRNE IP Study affirmed the existence of previously recognized gaps, such as those noted by the Government Accountability Office (GAO) in its August 2004 report “GAO-04-855, *Combating Terrorism: DoD Efforts to Improve Installation Preparedness Can Be Enhanced with Clarified Responsibilities and Comprehensive Planning*”, the Capability Based Assessment (CBA) for CBRN Defense, and the Quick Look Study for DoD CBRNE

Consequence Management (CM). The Study ultimately identified an overwhelming need for scalable capabilities built upon a foundation of DoD-wide standards and policy. The Study contains ten recommendations for improving CBRNE IP, seven of which deal with non-materiel issues.

The Study was briefed to the Joint Capabilities Board (JCB) on June 14, 2006. The JCB approved four key recommendations:

- The CBRNE IP program should adopt a three-tiered approach to fielding CBRNE capabilities.
- The Joint Staff should develop a prioritized list of installations to be used for fielding CBRNE IP program capabilities.
- DoD should implement recommended non-material solutions including, but not limited to: developing standards, revising policy, and increasing interoperability with civilian agencies. Additionally, DoD should integrate CBRNE IP issues into the military medical organizational structure.
- JPMG should deliver Tier 1 capabilities to installations through Fiscal Year 2011 (FY11), remaining within the currently programmed budget of \$375 million.

General Strategy. Charter a new CBRNE Installation Protection Steering Group (IPSG), co-chaired by the ATSD(NCB), the Assistant Secretary of Defense for Homeland Defense and Americas Security Affairs (ASD(HD&ASA)) and the Deputy Undersecretary of Defense for Installations and Environment (DUSD(I&E)). This steering group will manage the implementation effort by working with, and leveraging expertise and resources available through, the Services, Joint Staff, Defense Threat Reduction Agency (DTRA), Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD), Under Secretary of Defense (Policy) (USD(P)), Assistant Secretary of Defense (Health Affairs) (ASD(HA)) and others. The effort will leverage the results of the Study and will be synchronized with related current DoD wide efforts such as the Integrated Unit, Base, and Installation Protection (IUBIP) CBA, the WMD CM CBA, the Common Delivery of Installation Support (CDIS) initiative, and Joint Basing.

The IPSG will oversee efforts to develop and/or clarify two distinct levels or types of CBRNE IP standards. First, at the DoD level, policy will be established for an all-hazards installation emergency preparedness and management (EPM) program. This program will establish minimum installation preparedness and emergency response standards (excluding security and law enforcement activities) for all natural and technological disasters, as well as terrorist attacks. Also at the DoD (and Joint) level, current guidance for CBRNE IP will be revised to be directive and contain clear standards for safeguarding mission capability, personnel, and resources from the effects of CBRNE attacks based on vulnerability, mission criticality, and threat. These standards will contain measurable objectives and criteria and should (eventually) be linked to Common Output Level Standards (COLS) (as described in the draft Joint Base Implementation Guidance). These standards will enable an appropriate level of program decentralization, while maintaining compliance with public law and current policy regarding the development and procurement of chemical and biological defense equipment.

The second type of standards needed involve specific performance standards for CBRNE IP systems, such as personal protective equipment and detectors. These performance standards are dependent upon, and will be designed to support, the higher level standards described above. The Joint CBRND program will use existing capability development processes to develop these standards.

The implementation of both materiel and non-materiel recommendations will occur continuously during a three phase process. The first phase will establish the IPSPG charter; gather analysis from completed and on-going assessments; and begin revising DoD IP policy, including establishing the EPM program and defining risk-based CBRNE IP standards. The second phase will commence in mid FY08 and includes the development of key supporting pilot initiatives, system performance standards development, and independent validation and verification of standards in conjunction with other DoD initiatives. The final phase includes the refinement and the finalization of all policies, guidance, and standards in FY11.

Rationale. The personnel and the missions at DoD installations must be protected from a wide range of natural and manmade threats, including CBRNE attacks. The Study, GAO Report GAO-04-855, and the lessons learned from initiatives to improve DoD CBRNE IP, including the Joint Service Installation Pilot Project (JSIPP), the Unconventional Nuclear Warfare Defense Pilot Program (UNWD), the Navy First Responder Program, and the Air Force Weapons of Mass Destruction (WMD) Emergency Response Program, highlight the need for improved policy and standards for this area. The Department's inconsistent approach to all-hazards emergency preparedness and lack of clear CBRNE IP standards greatly inhibit the ability of the Department to ensure missions and personnel are protected from the full range of threats to installations.

The capability assessment conducted during the Study identified critical gaps and seams in the current execution of CBRNE IP. Of the 79 capability gaps identified in the assessment, 49 require non-materiel solutions; specifically new or revised DoD policies, standards, and Concepts of Operation (CONOPS) to support planning, organizing, resourcing, training, and conducting CBRNE IP operations. These gaps affect critical medical and non-medical capabilities. Closing these gaps requires coordinated action by policy offices outside of the USD(AT&L) and the JRO-CBRND.

DoD does not address "Installation Protection" through a single office with the scope of authority and requisite expertise to seamlessly integrate these key non-materiel CBRNE IP gaps into existing programs. Until "Installation Protection (from all-hazards)" is clearly defined, CBRNE IP remains a stove-piped process rife with gaps and overlaps. The Study observed that DoD organizations cannot effectively develop guidance to sufficiently resolve all installation-level gaps without improved policy, standards, and doctrine. DoD risks unnecessary redundancy and confusion at time of execution if these non-material gaps are not holistically addressed. Additionally, DoD does not have an efficient means for comparing and managing risks to installations globally across service and agency lines to enable effective resource allocation in support of national security and military strategies.

Intent. The IPSPG will be established to oversee, coordinate, and manage the Department's efforts to improve CBRNE IP. The IPSPG will serve as the focal point for all efforts to improve CBRNE IP and will report progress on achieving the goals in this action plan to the DepSecDef through USD(AT&L). The IPSPG will include key organizations such as the Services,

ASD(HD&ASA), ASD(HA), ASD Global Security Affairs (ASD(GSA)), ASD Special Operations and Low Intensity Conflict (ASD(SOLIC), USD(Intelligence), DTRA and JPEO-CBD. Strong leadership by the IPSTG Co-Chairs will be required to ensure the Department works aggressively to resolve these challenging issues. This approach will provide a central CBRNE IP focus until requirements are clarified, standards published, and CBRNE and all-hazards IP leadership roles and responsibilities are spelled out.

The IPSTG and the Joint Requirements Oversight Council (JROC) will provide oversight for ensuring the objectives in this action plan are met. The IPSTG will lead and monitor the overall effort, while the JROC will address applicable Joint Staff objectives through the Joint Capabilities and Integration Development System (JCIDS) management process outlined in CJCS Instruction 3170.E. IPSTG and Joint Staff efforts to improve CBRNE IP must be mutually supportive and coordinated.

The Joint Staff will use the JROC, the Joint Capabilities Board (JCB), the Force Protection Functional Capabilities Board (FCB), and the Combating WMD Working Group to address Doctrine, Organization, Training, Material, Leadership, Personnel and Facilities (DOTMLPF) gaps and other applicable non-materiel gaps. Objectives dealing with non-materiel capability gaps will primarily be addressed through the submission and implementation of joint DOTMLPF Change Recommendations (DCR) based on the capability assessment conducted during the Study and other relevant assessments, such as the Consequence Management Capabilities Based Assessment (CBA), Civil Support Analytic Baseline Study and Integrated Unit, Base, and Installation Protection CBA and Common Delivery of Installation Support (CDIS). The JRO-CBRND will identify capabilities and metrics for the CBRNE IP functional area, coordinate preparation of Joint CBRNE IP Defense capability documents, and provide assistance in the applicable policy and doctrinal areas.

Summary. The Study reaffirmed and clarified many previously known deficiencies in the Department's CBRNE IP program as well as the inherent limitations of a centrally managed program to resolve all of them. The key to addressing this situation is for the Department to establish clear policy and standards for CBRNE IP and institute an installation all-hazards emergency management program. Additionally, in the long-term, medical resources must be fully aligned to support antiterrorism and critical mission requirements for CBRNE attacks at installations. The objectives and tasks listed below lay out the path to establish an integrated standards-based IP program to protect DoD personnel and mission capability from CBRNE threats.

In addition to describing the overarching role of the IPSTG, this plan lays out specific objectives (derived from study recommendations) along with the tasks and estimated timelines to meet those objectives. Rough cost estimates for manpower necessary to accomplish initial planning and policy development, and to support the IPSTG are also listed. Cost estimates for full development and implementation of the objectives in this plan across the Department are not included. The overall objective should be accomplished as the program transitions to a standards based program. The resources required to execute this plan are contained in the baseline defense budget. The estimated level of effort (in work-years) required to accomplish the tasks in this plan are captured under each objective.

Objective 1. Establish a clear management structure, accountable for executing, monitoring, and coordinating issues and communicating results from this action plan.

(Lead: IPSTG Co-Chairs)

a. **Description.** The IPSTG will be responsible for this action. The IPSTG will identify and coordinate solutions for CBRNE IP capability gaps and actions required to transition CBRNE IP to a standards-based approach. The IPSTG will provide a venue to coordinate, integrate, and leverage the Department’s efforts in Antiterrorism (AT), CBRN defense, installation emergency preparedness and management, Fire and Emergency Services, medical, security/law enforcement, critical infrastructure protection, and consequence management in order to improve the readiness and resilience of DOD installations to CBRNE attacks. The IPSTG will:

- Be co-chaired by the ATSD(NCB), the ASD(HD&ASA), and the DUSD(I&E).
- Receive administrative support from the Office of the SA(CBD&CDP) (OSA(CBD&CDP)).
- Report progress on the implementation of this action plan to the DepSecDef through the USD(AT&L).
- Coordinate closely with the FP FCB and the JCB on CBRNE IP issues.

The IPSTG will provide written reports to the DepSecDef, through USD (AT&L), on the Department’s progress towards completing the objectives in this action once every six months for a period of three years, or until all objectives have been completed, whichever is sooner.

b. Plan of Action.

Task	Action	Office of Primary Responsibility (OPR)	Start Date	Completion Date or Frequency
1.1	Draft Charter for Installation Protection Steering Group (IPSTG)	OSA(CBD&CDP)	Ongoing	Jun 07
1.2	Vet charter among key stakeholders	OSA(CBD&CDP)	Jun 07	Jul 07
1.3	Submit charter USD(AT&L) for formal approval	OSA(CBD&CDP)	Jul 07	Jul 07
1.4	Identify key members by position	OSA(CBD&CDP)	Jul 07	Jul 07
1.5	Conduct first meeting of IPSTG	OSA(CBD&CDP)	Jul 07	Jul 07
1.6	Develop draft prioritized IPSTG task list	OSA(CBD&CDP)	Jul 07	Jul 07
1.7	Submit draft prioritized IPSTG task list to IPSTG co-chairs	OSA(CBD&CDP)	Jul 07	Jul 07
1.8	IPSTG co-chairs approve prioritized task list	ATSD(NCB)	Aug 07	Aug 07
1.9	Conduct meetings to address capability gaps and monitor progress toward CBRNE IP Action Plan objectives	OSA(CBD&CDP)	Jul 07	monthly
1.10	Provide updates to the FP FCB	OSA(CBD&CDP)	Aug 07	quarterly
1.11	Provide updates to the USD(AT&L)	OSA(CBD&CDP)	Aug 07	as needed

1.12	Report progress to DepSecDef	IPSG co-chairs and USD(AT&L)	Aug 07	semi-annually
------	------------------------------	------------------------------	--------	---------------

c. **Level of effort.** 1.5 work-years annually at OSA(CBD&CDP) for 3 years.

Objective 2. Define an all-hazards installation emergency management program that incorporates CBRNE IP concepts with guidance and standards for all aspects of emergency preparedness, mitigation, response, and recovery including training, exercising, planning, resourcing, interoperability with civilian responders, and integration with other existing programs.

(Co-Leads: USD(AT&L) & USD(Policy) (USD(P))

a. **Description.** USD(P) and USD(AT&L) will coordinate and standardize DoD installation emergency management and response to enhance the Department’s ability to safeguard personnel, missions, and critical infrastructure from all-hazards, including CBRNE. USD(P) will provide directive guidance to establish a DoD Installation Emergency Management Program (IEMP). This guidance will direct a comprehensive approach to managing strategic risks to DoD operations and personnel by reducing the vulnerability of installations to natural and technological disasters, including the impacts of terrorist CBRNE attacks. Risk management will be directly linked to tiered definitions of mission criticality that support development of attainable, risk-based capability standards for protecting personnel and providing mission assurance. USD(P) and USD(AT&L) will coordinate closely to ensure that mission definitions and standards are adequately developed and validated to support implementation of a standards-based program by 2011. JPEO-CBD will support OSD by assuming the principle role in developing and coordinating the materiel standards and specifications as the legally designated life-cycle manager for CBD materiel.

USD(AT&L) will implement the IEMP through a DoD instruction (DoDI) establishing minimum installation-level standards for the full spectrum of emergency preparedness activities, including training, exercising, planning, resourcing, establishing interoperability with civilian responders, and integrating IEMP with other installation programs. The IEMP DoDI will specify required CBRNE IP capability levels linked to the mission guidance to support the mission definitions provided by USD(P). The Services, DoD Agencies, and Combatant Commands (COCOMs) will implement the IEMP throughout all commands and agencies at DoD installations.

The IEMP DoDI will provide directive guidance on emergency response capability levels required to support the mission definitions provided by USD(P). This new DoDI will be similar in scope and format to DoDI 6055.6, *Fire and Emergency Services Program*, published by DUSD(I&E). Regarding CBRNE IP, the IEMP DoDI will, at a minimum provide standards for:

- Installation emergency management and response operations plans.
- Training, exercises, and assessments.
- Emergency Operations Centers.
- Installation warning and mass notification systems.
- Protection of personnel from CBRN hazards and environments through the use of protective equipment, collective protection, sheltering in-place, and evacuation.

- Detection, identification, and marking of CBRN hazards.
- Hazard prediction and modeling.
- Mass decontamination.

b. Plan of Action.

Task	Action	OPR	Start Date	Completion Date or Frequency
2.1	Discuss issue at IPSTG	OSA(CBD&CDP)	Jul 07	Ongoing
2.2	Define scope and depth of policy document requirements	USD(P) and USD(AT&L)	Jul 07	Sep 07
2.3	Assign “primary author” for new/revised policy documents	USD(P) and USD(AT&L)	Jul 07	Sep 07
2.4	Detailed outline of new/revised documents to IPSTG for review	USD(P) and USD(AT&L)	Jul 07	Oct 07
2.5	Draft documents for stakeholder comment	USD(P) and USD(AT&L)	Aug 07	Dec 07
2.6	Formal Coordination	JS, Services, Agencies, and COCOMs	Dec 07	Mar 08
2.7	JS, Services, Agencies and COCOMs identify DOTMLPF impacts of IEMP	JS, Services, Agencies, and COCOMs	Dec 07	Mar 07
2.8	JS, Services, Agencies, and COCOMs develop or revise policy, doctrine, training, and organizations as needed to comply with new DoD IEMP	JS, Services, Agencies, and COCOMs	Mar 07	May 08
2.9	JS, Services, Agencies, and COCOMs implement IEMP	JS, Services, Agencies, and COCOMs	May 08	N/A

c. **Level of effort.** 2 work-years annually at DUSD(I&E) for 3 years.

Objective 3. Improve integration of DoD CBRNE IP capabilities with National Capabilities.

(Lead: USD(P))

a. **Description.** DoD will work with the Department of Homeland Security and the Homeland Security Council Policy Coordinating Committees (HSC/PCCs) to ensure DoD capabilities and standards are interoperable with National standards and procedures. CBRNE events affecting installations will require mutual aid and an interagency response. Currently, some DoD procedures and CONOPS differ from the DHS standardized approach. By examining interoperability early on, DoD can increase its efficiency and effectiveness through interoperability with local capabilities. Specific areas of emphasis include the following:

- Understanding of, and integration of BioWatch and Domestic Nuclear Detection Office capabilities/information networks with DoD installation protection activities.
- Coordination and integration of OSD and DHS policies, plans, procedures, technology for CBRNE incident preparedness, response, management, and recovery.
- Interoperability of emergency operations, at the Federal, State and local levels, including communications protocols and equipment.

USD(P) will also ensure effective DoD-wide implementation of the National Incident Management System (NIMS) and support efforts to integrate military and civilian CBRNE incident management assets, including installation of Mutual Aid Agreements (MAA) with local, state, and federal response agencies.

b. Plan of Action

Task	Action	OPR	Start Date	Completion Date or Frequency
3.1	Identify operational CBRNE Incident Reporting Procedures	USD(P), Joint Staff	Ongoing	Aug 07
3.2	In collaboration with Homeland Security Counsel (HSC), determine which DoD offices should attend HSC/PCC and other agency meetings	ASD(HD&ASA)	Ongoing	Jun 07
3.3	Attend HSC/PCC meetings and coordinate DoD positions on DoD/civilian domestic CBRNE issues.	ASD(HD&ASA)	Ongoing	Ongoing
3.4	The Non-Standard Equipment Review Panel (NSERP) will specifically address CBRN IP and Defense Support to Civil Authorities interoperability in equipment reviews	JPEO-CBD	Jun 07	Ongoing

c. Level of effort. N/A

Objective 4. Standardize emergency management doctrine and prioritize installations.

(Lead: Joint Staff)

a. **Description.** The National Incident Management System (NIMS) and National Response Plan (NRP) provide overarching guidance for federal, state, and local governments to work effectively and efficiently to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. The JRO-CBRND will ensure that joint CBRNE IP concepts and capability documents support NIMS and the NRP and are integrated into Joint Future Operational Capabilities. The Joint Staff and Combatant Commanders (COCOM) will standardize emergency management by developing/revising Joint Publications, Multiservice Tactics, Techniques, and Procedures (MTTPs) and concepts of operation (CONOPS) for DoD installation response procedures. The JPEO-CBD and DTRA will ensure that materiel architectures and efforts for installation protection support the NIMS and the NRP. Additionally,

the Joint Staff will produce a prioritized list (for approval by SecDef) of installations to receive the tiered CBRN capability packages. This list will be produced in collaboration with the Services and COCOMs and be delivered to the JPEO for fielding and execution.

b. Plan of Action.

Task	Action	OPR	Start Date	Completion Date or Frequency
4.1	Coordinate preparation of Joint CBRN IP Defense requirement documents	JRO CBRND, Services	Ongoing	Ongoing
4.2	Integrate CBRN IP Requirements into the Joint Future Operational Capabilities list and advise the Science and Technology community.	JRO CBRND	Jun 07	Annually
4.3	Develop/revise the MTTPs for Installation CBRN Defense in concert with NIMs and NRP (All-hazards framework).	JRO CBRND	Ongoing	Jul 07
4.4	Joint Staff, in coordination with ASD (HD) assesses the need/validity of DOD Interim CONOPS based on the development of MTTP for Installation CBRN Defense and JP 3-41 CBRNE Consequence Management	JRO CBRND, ASD (HD)	Jul 07	Dec 07
4.6	J34 identifies DOD critical assets	Joint Staff J34	Ongoing	Mar 07
4.7	Joint Staff, in coordination with the Services, COCOMs and JPMG will recommend a prioritized list of DOD Installations/facilities for CBRN IP Tiered Capability Packages	Joint Staff	Ongoing	May 07

c. Level of effort. 2 work-years annually at JRO-CBRND for 3 years.

Objective 5. Integrate medical requirements for CBRNE-IP into the overall military health system.

(Lead: Assistant Secretary Defense (Health Affairs) (ASD(HA)) through Tricare Management Activity (TMA) and Service Surgeons General (SG))

a. Description. An efficient and effective medical response is imperative for the management of a CBRNE event. However, the CBRNE IP mission is not institutionalized in the military medical community's organizational structure. There are inadequate CBRNE IP standards for medical treatment facilities (MTFs), and no comprehensive CBRNE training or exercise programs are available. Moreover, the military medical community has not adequately planned for coordinated participation in emergency operations centers (EOCs). To meet this objective, the military health system (consisting of ASD(HA), TMA and the Service SG) will identify and

integrate medical requirements for CBRNE IP, in coordination with the Joint Staff, COCOMs, civilian medical community, and other stakeholders.

Many installations lack the organic first responder/first receiver medical capabilities to support CBRNE IP. DoD must address requirements for more robust capabilities and engage civilian counterparts to appropriately address gaps where they exist. Consequently, the Military Departments must develop uniform response capabilities that facilitate integration of multi-service and civilian response resources. In order to provide a comprehensive protection capability, installation plans must incorporate health service support and force health protection requirements (i.e. fixed MTF and deployable capabilities). The DoD must also address the unique challenges of isolation, quarantine, shelter in place, and fatality management during a CBRNE event.

The DoD should ensure this effort is done in close coordination with the efforts of NORTHCOM and ASD(HA). One key avenue for coordination is through the NORTHCOM chartered Force Health Protection-Military Homeland Defense Working Group (with participation as needed by other COCOMS). The IPSPG will monitor and guide these efforts. Once standards are established, USD(Personnel & Readiness) (USD(P&R)), will take action to ensure appropriate medical staffing and resources are provided to meet CBRNE IP capability requirements.

b. Plan of Action

Task	Action	OPR	Start Date	Estimated Completion Date
5.1	Develop Medical CBRNE IP mission assurance standards	USD(P), ASD(HA), Joint Staff	Jun 07	Jul 08
5.2	Define Medical CBRNE IP requirements	Joint Staff	Jun 07	Dec 08
5.3	Ensure the military health system is organized and resourced according to CBRNE IP doctrine and policy	Services	Jun 07	Dec 11
5.4	Develop medical surveillance standards and requirements	ASD(HA), Joint Staff	Jun 07	Dec 07
5.5	Validate medical CBRNE IP material solutions with task standards	JPEO-CBD, Joint Staff/JRO CBRND, Services	Aug 07	Dec 08

c. **Level of effort.** 2 work-years annually at ASD(HA) for 2 years.

Objective 6. Implement a three-tiered approach to fielding CBRNE Installation Protection capabilities in the near-term.

(Lead: JPEO-CBD)

a. **Description.** On 13 October, 2006, OASD(CBD&CDP) issued interim program guidance for the IPP to JPEO-CBD to initiate the fielding of tiered CBRN installation protection and response capabilities for military installations as identified in the study.

Effective risk management demands concentration of resources in areas of highest risk. Before fielding CBRNE IP capabilities, vulnerability and threat assessments should be examined to identify the level of capability needed. The IPP serves as a strategic risk mitigation effort and capability bridge to provide enhanced defensive capability and reduce DoD installation vulnerability from CBRNE terrorist attacks until DoD transitions to a standards-based CBRNE IP program. It is critical the program provide an integrated capability that preserves the ability to sustain critical missions, protect installation personnel (both as a deterrent and to safeguard of combat power), and serves as a bridge to future capabilities. JPEO-CBD will:

- Given the changing threat and evolving Department needs, implement a tiered approach acquisition strategy.
- Develop the support tools necessary to establish the Baseline Tier to support implementation by FY08.
- Maintain the Tier 2 architecture and field the capabilities to a limited number of bases
- Field CBRNE IP capabilities in accordance with the Joint prioritized list of installations.
- Provide JPEO-CBD expertise, lessons learned, and assessment opportunities to support the development of the end-state, standards-based program.
- Support the IPSG by leading (in concert with the CBRNE IP community) the development and validation of materiel solution standards for CBRNE IP.

b. Plan of Action

Task	Action	OPR	Start Date	Completion Date
6.1	Issue Interim Guidance Memo directing JPMG to implement tiered approach for IPP	OSAD(CBD&CDP)	Completed	Completed
6.2	Implement Milestone Decision Authority approved revised Acquisition Strategy	JPEO CBD	Completed	Completed
6.3	Formal DepSecDef approval of CBRNE-IP Plan	OSAD(CBD&CDP)	Jun 06	May 07
6.4	Provide tiered capabilities based on requirement documents, standards, study recommendations and Joint prioritized list of installations.	JPEO CBD	Oct 06	Sep 11
6.5	Generate supporting POM documentation for FY10 POM build	JPEO CBD	Jul 07	Feb 08

c. Level of effort. N/A