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

APR 24 2006

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Policy on Discussion of IEDs and IED-Defeat Efforts in Open Sources

Public and media interest in the Improvised Explosive Device (IED) threat, IED-defeat efforts, and the Joint IED Defeat Organization (JIEDDO) remains high. Reporters contact the JIEDDO, Service public affairs offices, individual commands, and service members on a daily basis for information, imagery, and interviews. Furthermore, as we work together to defeat this threat, information is continuously requested and shared within and between the Services, government organizations, academia, the research community, and industry.

While Department of Defense policy is to share information to the greatest extent possible, such access must be balanced with careful consideration of operational security. The enemies we face are adaptive and innovative, and they glean substantial information from open sources. Individual pieces of information, though possibly insignificant taken alone, provide robust information about our capabilities and weaknesses. There is very strong evidence that our enemies study our media, web sites, and private, professional, and technological forums to gain insights into our operational understanding and practices. Their ability to exploit our open source information is multiplied by their ability to rapidly disseminate information on the World Wide Web.

Divulging sensitive information about IEDs compromises the safety of our Soldiers, Sailors, Airmen, and Marines. Therefore, members of the Department should restrict their comments on the IED threat or IED defeat initiatives to the points listed in Annex A of this memorandum. They should not comment on the subject without specific authorization, but should refer further questions to DoD Public Affairs and the Joint IED Defeat Organization (JIEDDO). Specifically protected IED information is shown in Annex B.

Preserving information security is a critical component to winning this war and protecting the lives of our service members. Please ensure widest possible dissemination of this policy throughout your organizations.

Gordon England 4/24

Attachments:
1. Annex A: Approved IED Talking Points for All Personnel
2. Annex B: Specifically Protected IED Information

Annex A

Approved IED Talking Points for All Personnel

- The IED threat and its defeat is a top priority for DoD.
- DoD is devoting significant resources (equipment, personnel, tactics, training, and procedures) to defeating IEDs.
- The Joint IED Defeat Organization works with the Services and all of DoD to develop integrated solutions that balance intelligence, training, and technology.
- The IED issue is a complicated one, and no single solution exists to defeat IEDs. Our strategy includes three components:

  1. Training is paramount. The best sensor and weapon on the battlefield is a well-trained, situationally aware Soldier, Sailor, Airman, or Marine.
  2. Killing or capturing bomb makers and disrupting or eliminating their networks is vital.
  3. Providing troops on the battlefield with effective, innovative technology enables the fight.

Annex B

Specifically Protected Information

The following types of information should not be released in open sources:

- Our specific knowledge of enemy IED tactics, techniques, and procedures, and our analysis of enemy capabilities or vulnerabilities.
- Friendly force equipment, technological, organizational, or operational vulnerabilities.
- Specific friendly force technology areas or details, organizational initiatives, and operational procedures designed to counter IEDs.
- Specific exploitation tactics, techniques, and procedures.
- Photos of or information about vehicles or equipment that have been damaged by an IED.
- Photos of or information about recovered components of an IED.
- Locally produced briefings should be classified. The minimum level of classification for any briefing or document related to IED Defeat is UNCLASSIFIED FOR OFFICIAL USE ONLY. The association of any of this information with deployed troops or specific locations will normally mean it should be classified much higher and afforded a greater level of protection.
- Briefings that are designed to impart information to service members who are preparing for deployment generally are not suitable for presentation or release to media.
- IED Countermeasures consist of technology solutions as well as operational procedures, organizational, and doctrinal initiatives. All must be protected.