# Responses to FAS Query from Mr. Robert Rogalski, Director of Security, Deputy Undersecretary of Defense (Counterintelligence and Security)

**Q1**: It appeared to me that portions of the Taguba report on Abu Gharib were unnecessarily and wrongly classified, i.e. that they violated the limitations on classification prescribed in Executive Order 12958. Was the Taguba report improperly classified? Has its classification status been modified?

**A1**: At the time the decision was made, it was based on the standards provided in Executive Order 12958, as amended—specifically, military operations, intelligence activities, and foreign relations/activities. As of October 15, 2004, the majority of the Taguba Report was declassified. This underscores the point that DoD has a process in place that provides oversight.

**Q2:** Does the department acknowledge that over-classification occurs? If so, what are the causes of over-classification? What are the consequences?

**A2:** Yes, we agree that there are issues related to excessive classification and that's why we have processes in place to ensure classified data can be reviewed and declassified. The fundamental principle of classification is to ensure the protection of information the release of which will not undermine or jeopardize national security. However, the need for proper secrecy must be balanced with openness that is fundamental to our democracy. The over classification was not done with malfeasance, but as a result of the tempo of operations, lack of training and oversight. DoD information is not classified or otherwise withheld from public disclosure to protect the government from criticism or embarrassment.

**Q3:** What steps, if any, is the Department taking to combat over-classification and to ensure the integrity of classification policy and practice?

**A3:** We need to continue to aggressively pursue clarifying the policies and educating the people who must implement them. Here are some of the actions we're taking:

- The Secretary of Defense, on September 16, 2004, conveyed a message to DoD his personal commitment to a strong information security program, reminding classification authorities of their responsibility to properly classify information.
- On October 5, 2004, the Director of Security for DoD chaired a meeting of the DoD Security Directors Group consisting of senior security personnel from the Military Departments, Defense Agencies and Combatant Commands and emphasized their responsibility to have a strong classification management program.
- A DoD Director of Security video emphasizing classification management is in development. It will be sent throughout DoD for organizations to use in their security awareness program.

- Updating classification guidance and making it available to those who need it.

- Modifying security education and training so that it focuses more on when and why it is appropriate to classify information and developing web-based training that will be available to all within the Department.

- Conducting security reviews to determine if information has been appropriately classified.

- Keeping the number of original classification authorities to a minimum.

- Conducting periodic self-inspections to review the classification management program.

- DoD agencies are also periodically inspected by the Information Security Oversight Office to ensure proper classification management principles are followed.