WRITTEN STATEMENT
For
HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS
"DROWNING IN A SEA OF FAUX SECRETS: POLICIES ON HANDLING OF CLASSIFIED AND SENSITIVE INFORMATION"
(March 14, 2006)

Good afternoon, Chairman Shays, Congressman Kucinich, and distinguished members of the subcommittee.

I appreciate the opportunity to discuss the Department of Defense's (DoD) policies and practices with regard to the identification and safeguarding of classified national security information and controlled unclassified information (CUI).

Within DoD, my office is responsible for developing policies that address both classified and controlled unclassified information. This responsibility is executed on behalf of the Secretary of Defense and the Under Secretary of Defense for Intelligence who is the Department's designated Senior Agency Official (SAO) in accordance with Executive Order (EO) 12958, as amended, "Classified National Security Information."

My discussion today will focus on the Department's policies on CUI, the draft Government Accountability Office (GAO) report No. 06-369 entitled, "MANAGING SENSITIVE INFORMATION: Departments of Energy and Defense Policies and Oversight Could Be Improved," classified information (to include reclassification) and, finally, the relevance and efficacy of current regulations, guidance, training and procedures that govern classification, reclassification, and the application of CUI designations, including the use of the FOUO (For Official Use Only) marking.

CUI POLICY

"Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations." This is a direct quote out of the preamble to Executive Order 12958, as amended, "Classified National Security Inforfmation." This same concept, to a lesser degree, also applies to controlled unclassified information.

The Department of Defense uses the generic term "controlled unclassified information" (CUI) to refer to all unclassified information that has been determined to require, for various reasons, some type of protection or control. This information is often called "sensitive but unclassified" (SBU) information by others. Because of the large volume of information that may be CUI, the initial identification and designation as CUI is done by the individual who generates a document.

FOUO is the largest category of CUI within the DoD. Documents are marked FOUO when the information is deemed by the originator to be potentially eligible for withholding from public release if requested under the Freedom of Information Act (FOIA) (Section 552 of Title 5, U.S.C., as amended) exemptions 2 through 9.

At this point it is important to note that marking CUI serves to inform DoD personnel that the information may qualify for withholding from public release and it requires some degree of safeguarding. It does not mean it is automatically withheld without review. All DoD information, whether marked as CUI or not, is specifically reviewed for release when public disclosure is desired by the Department such as a security review or requested by others under the provisions of the FOIA. Any erroneous

designation as FOUO is identified and corrected in this review process and the information released as appropriate. Thus, information is not withheld from public release based solely on the initial markings applied by the originator. The Department has an extensive appeal process to ensure that release is done based on appropriate criteria.

CUI also has specific safeguarding requirements which are less stringent than what is required for classified, for example, store in a locked desk drawer versus a General Services Administration (GSA) certified security container and, when in a network environment, Information Technology controls are correspondingly less restrictive.

However, we do believe improvements can be made in how we handle CUI as mentioned in the GAO Report.

DRAFT GAO REPORT

In our official February 7, 2006 response to GAO, we agreed with their recommendation to clarify policy regarding the use of the FOUO designation, which is one of our primary subcategories of CUI, and including it in our oversight activities. We also agreed with the need for more robust training. However, we disagreed with placing the applicable

FOIA withholding exemption on the document when it is first created. Besides the fact that FOIA exemptions are not determined until the document is requested under the FOIA, this could create problems if the wrong exemption was cited. It is then possible that other documents that are derivatively created from this document would also carry the incorrect FOIA exemption or that the incorrect designation could cause problems if a denial is litigated. Also, due to the possibility of FOIA exemptions not being applicable over the passage of time, not designating FOIA exemptions on documents would ensure the greatest possible release to the public.

CLASSIFIED NATIONAL SECURITY INFORMATION POLICY

Classification is a challenge because of the balance that must take place between the need for proper safeguarding and the need for openness that is fundamental to our democracy. While we understand the need for openness we also have a responsibility to the American public to protect information that ensures our continued freedom. We in the Department also have the added challenge of ensuring good classification principles are applied in a high tempo operational environment. We may sometimes take a more conservative approach to classification so as not to endanger personnel and operations. That is why the Department is committed to ensuring that our

classifiers take their responsibility seriously, are well trained, and are accountable for their actions.

The identification and designation of classified information is accomplished according to the classification criteria in EO 12958, as amended, by trained original classification authorities (OCA) having functional responsibility over the information. The decision making process is a best judgment based on all of the variables at the time an original decision is made. Key to the decision is whether release of the information would cause damage to national security. That is why we have implemented rigorous training requirements for the original classifiers so that they fully understand the classification process and their responsibilities, to include the prohibitions. The Department has a large number of classification guides codifying original classification authority decisions.

Declassification of classified information occurs when the appropriate OCA determines that the information can no longer cause damage to national security. Declassification reviews are prompted by a number of things, to include: requests for mandatory declassification review; records eligible for automatic declassification; Freedom of Information Act (FOIA) requests; and, in the event of actual or possible compromise of information. Another

key declassification activity is the completion of our review of records eligible for automatic declassification by December 31, 2006. In addition to the automatic declassification provisions of Executive Order 12958, as amended, the Secretary of Defense has directed we make every effort to declassify information as soon as it no longer meets the criteria for classification.

As set forth in Executive Order 12958, as amended, agency heads, are permitted to reclassify information in certain circumstances. However, DoD rarely exercises this option. For example, since the establishment of the Under Secretary of Defense for Intelligence in 2003, he has only reclassified information once.

Essential to effective implementation of the classification management program is training and oversight. All personnel who are cleared and handle or generate classified information are trained on their responsibilities. The purpose of the Defense Security Service Academy is to train our security professionals who in turn train personnel throughout DoD. I invite you and your staff to visit the Academy at Linthicum, Maryland. Additionally, oversight is directed to occur at every level of the Department to ensure classified information is correctly identified and marked, appropriately safeguarded, and declassified at the earliest possible date.

RELEVANCE AND EFFICACY OF CURRENT CLASSIFICATION AND CUI POLICY

All of our security policies have come under close scrutiny to ensure they are clear, consistent, relevant, efficient, and do not impede the necessary sharing of information. The Department is also involved in national efforts to do the same. We are participating in the Information Security Oversight Office revisions to EO 12958, as amended, to address the Weapons of Mass Destruction Commission recommendation regarding information sharing and the Department of Homeland Security's efforts to standardize CUI procedures for terrorism, homeland security and law enforcement in response to the requirements of Section 1016(D) of the Intelligence Reform and Terrorism Prevention Act (IRTPA).

There are a number of things the Department has done to clarify and emphasize classification management already:

- **The Secretary conveyed a message to all DoD Components of his personal commitment to a strong information security program,**

reminding classification authorities of their responsibility to properly classify information. He also prohibited the use of drafts and working papers as sources for derivative classification.

- **The Under Secretary of Defense for Intelligence, DoD's senior agency official, subsequently issued training requirements for original and derivative classifiers. The Department's goal is to ensure there is a uniform thought process applied to each classification decision.**

- **The Under Secretary of Defense for Intelligence requested a review of positions requiring original classification authority. While we have reduced some, we will continue the campaign to reduce them even further.**

- **The DoD Director of Security chairs a meeting of the DoD Security Directors Group quarterly consisting of senior security personnel from the Military Departments, Defense Agencies and Combatant Commands and emphasizes, among other things, their responsibility to have a strong classification management program.**

- **The DoD Director of Security conducted a video broadcast emphasizing classification management that was made available to all DoD Components through the Defense Security Service Academy news network.**

- **The Department conducted oversight visits of Combatant Commands with ISOO to determine if information had been appropriately classified, and made classification management a point of emphasis during outbriefs with the senior leadership.**

- **We continue to work with Defense Security Service Academy on updating and reinforcing the training requirements which are key to a successful program. The Defense Security Service Academy has been working on new training courses to further enhance classification and declassification, to include computer-based training that will be more accessible to a larger audience.**

- **DoD is establishing a certification program for its security professionals which will include training in classification management.**

- **We chair a DoD Declassification Management Panel of DoD Components to share best practices, learn about problems, and plan the future of DoD's declassification efforts.**

We just conducted a DoD-wide security managers' conference last week where we were able to convey to an audience of approximately 800 security professionals updates and reminders on classification management and CUI policies.

Also, the Department is conducting a study to help develop security policy for the 21st century. As part of that study, we will look at what professionals from various sectors outside the Department, such as academia and industry, are doing to safeguard information.

In closing, the Department has solid foundational policies in place that are still relevant and on which we can continue to build. We have also accomplished much to bring education and emphasis to important classification management issues to reduce overclassification. Furthermore, the Department will pursue increased training on CUI. The Department takes its responsibility seriously and continues to strive to reach the right balance between properly safeguarding and the need for openness that is fundamental to our democracy.

Again, I thank you for the opportunity to brief you on the Department's policies and look forward to the discussions on this important topic.