

**STATEMENT FOR THE RECORD**

**BY**

**MS CAROL A. HAAVE**

**DEPUTY UNDER SECRETARY OF DEFENSE  
COUNTERINTELLIGENCE AND SECURITY**

**BEFORE THE**

**SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING  
THREATS AND INTERNATIONAL RELATIONS**

**COMMITTEE ON GOVERNMENT REFORM**

**U. S. HOUSE OF REPRESENTATIVES**

**AUGUST 24, 2004**

## INTRODUCTION

Mr. Chairman, members of the Committee. Thank you for the opportunity to speak with you about the Department of Defense's classification management program and what we are doing to protect classified information while fostering an environment that allows extensive sharing without compromising critical sources and methods or operations. It is a delicate balance that we strive to achieve, one that is important for the Government and the public it represents.

## BACKGROUND

National concern about protecting "secrets" was codified in 1917 when the Congress passed the first Espionage Act. At that time violations of the law could result in "punishment by a fine of not more than \$10,000 or by imprisonment for not more than two years, or both" -- presumably a serious consequence in those days. Since then, we have continued to affirm the need for such laws to classify information deemed critical to the security of the United States, although they have remained relatively unchanged since 1940 when President Roosevelt signed Executive Order 8381 creating three levels of classification and specifying the "authorities" as to who could classify information. Over the subsequent decades, changes have been made that reflect the Government's, either more liberal or conservative philosophy about "secrets." Today, Executive Order (EO) 12958, "Classified National Security Information" as amended recently by EO 13292 governs how we classify, safeguard and declassify national security information.

## THE DEPARTMENT OF DEFENSE PROGRAM

Within the Department of Defense, we implement classification and declassification policies through the DoD 5200.1-R, "Information Security Program Regulation," most recently updated in April 2004. That regulation is based upon the EOs cited above, as well as the Information Security Oversight Office (ISOO) Directive Number 1, "Classified National Security Information." In 1998 DoD and the Central Intelligence Agency (CIA) agreed to have uniform lexicon and methodology for showing classification markings. That methodology is captured in the Intelligence Community Classification and Control Markings Register.

There are two types of classifiers – original classification authorities (OCA) and derivative classifiers. OCAs are senior ranking officials within the Department who have been delegated the authority to classify information over which they have jurisdiction. For example, the Secretary of Defense, the Chairman of the Joint Chiefs of Staff and the Under Secretary of Defense for Policy have the authority to classify information up to Top Secret\*. Those who use or restate information originally classified by one of the above are required to apply the original classification guidance. OCAs can assign one of three levels of classification to information – Confidential, Secret, or Top Secret. The level is determined by the seriousness of the damage that would be caused if the information were compromised. Additionally, there are program access designations and dissemination control markings\*\* such as “Not Releasable to Foreign Nationals” (NOFORN) and “Dissemination and Extraction of Information Controlled by Originator” (ORCON) that further limit the extent to which information may be shared.

According to the EO, information pertaining to military plans, weapons, operations, intelligence activities, scientific and technological matters, vulnerabilities or capabilities of systems and foreign government information may be classified, if its disclosure would be injurious to the nation’s security. The decision to classify, or not, certain information is a risk determination. OCAs develop classification guides (similar to handbooks) that indicate what information about a system, plan, program or project is classified and the appropriate markings that are to be used. Within the Department, we have an index of about 3000 classification guides. For example, there are classification guidelines for Operation Enduring Freedom and Iraqi Freedom, as well as most acquisition programs.

Since 9/11, and in times of war, it is not inconceivable that more information would be classified. However it should also be noted that the Department of Defense is also responsible for almost half of the information that has been declassified since 1995.

\* Sensitive Compartmented Information (SCI) is the purview of the Director for Central Intelligence (DCI) in accordance with (IAW) DCI Directive (DCID) 6/1.

\*\* Dissemination markings are also under the purview of the DCI IAW DCID 6/6.

One key concern in this discussion is that of unauthorized public disclosures of classified information. This unilateral, unapproved declassification compromises sources and methods, which damages intelligence and operational capabilities, may result in loss of life, breaches with cooperating governments and reveal dangerous vulnerabilities of US persons, US installations and this country. These lessen the Department's ability to protect critical information, technologies and programs—and they appear to be increasing at an alarming pace. Unauthorized disclosures demoralize those who are adhering to the standards of classification and their security agreements, has the potential to minimize the return on investment of taxpayer dollars when science and technology advantages are compromised, and may put the nation at risk. The Department continues to assess and improve its security education, training and awareness program to address this and other important security matters.

The DoD has an active classification management oversight program that is conducted de-centrally at multiple levels throughout the Department. Components are responsible for ensuring that OCAs are trained, conducting self-inspections to ensure compliance and providing information annually about the state of their classification management efforts to the Office of the Secretary of Defense (OSD) and ISOO. At the OSD level, oversight consists of providing classification management training coursework and conducting program, security and classification guidance reviews.

In the future, one could envision the process of classification and declassification to be easier. It will still require that people classify information appropriately. This is a training issue and the Department is creating an updated, web-based course accessible by all who need it. It will also require that we recognize the need for seamless availability and integration of multiple levels of classified and unclassified information among Federal, state, local and other organizations. Data from each of these entities are governed by their own unique statutory requirements.

The Department of Defense has embraced the 21<sup>st</sup> century information technology revolution. We are deploying the Global Information Grid, an enterprise architecture, to network all users in a common environment and with common services. We are mandating metadata and other standards to facilitate sharing across networks and among applications to foster collaboration and situational awareness. We are continuing to research and employ the latest technological advances, i.e., Internet protocol (IP)-based,

high speed, bandwidth on demand, and are investing heavily in persistent-continuous Information Assurance. We are developing cross-domain security solutions that will allow information to flow seamlessly between multiple classification levels. We have established a worldwide Public Key Infrastructure (PKI) for “trusted” network access control and user authentication for over three million DoD personnel as well as a PKI Federal Bridge to facilitate interoperability across the Federal Sector that includes contractors and vendors. The vision is a user-driven, “smart-pull,” highly trusted and networked, seamless, cross security domain environment that allows cooperation and collaboration among those who have been properly vetted. And while there is much being done, there is much more to do.

The decision to classify or not is a risk decision and not one the Department takes lightly. We continuously strive to balance the public’s desire for information with the protections necessary to ensure the safety and security of our nation that is more at risk today than ever before.

I thank you for the opportunity to address this critical challenge.