STATEMENT BY

MAJOR GENERAL THOMAS B. GOSLIN, JR., USAF

DIRECTOR OF OPERATIONS, UNITED STATES SPACE COMMAND

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

EMERGING THREATS AND CAPABILITIES

INFORMATION ASSURANCE

1 MARCH 2000

Mr. Chairman and members of the Subcommittee:

On behalf of the Commander in Chief of United States Space Command (USCINCSPACE), I am pleased to have the opportunity to discuss the subject of Information Assurance (IA) as it relates to United States Space Command (USSPACECOM) operations.

The President's 1999 Unified Command Plan (UCP) assigned USCINCSPACE responsibility for Computer Network Defense (CND), effective 1 October 1999. In addition to conducting CND operations, USCINCSPACE also has the responsibility and authority to support all other Commander in Chiefs (CINCs) to plan, develop and advocate national requirements for CND.

The formal move to place responsibility for CND under a CINC highlights the recognition by our nation's leaders that we must rapidly improve joint operations in order to protect and defend our critical DoD Information Infrastructure (DII). Several factors make this necessary as we enter the 21st century.

Joint Vision 2010 aims to achieve the four operational concepts of dominant maneuver, precision engagement, full dimensional protection, and focused logistics. These concepts encompass a broad array of capabilities required to meet the challenges of the 21st century. However, to achieve these capabilities, our joint forces must be able to maintain Information Superiority. We must place special emphasis on the importance of defending our information systems in order to attain and sustain Information Superiority.

Today, a broad range of threats exists to our information infrastructure, and therefore to our ability to maintain Information Superiority. In addition to these threats, USSPACECOM has become increasingly aware of certain vulnerabilities inherent in our current Defense Information Infrastructure (DII). Our concern is heightened because any adversary will look for ways to exploit our vulnerabilities and most likely apply asymmetric strategies to exploit or attack our defense networks and reduce the United States' ability to maintain Information Superiority. We believe that "cyber aggression", as part of an adversary's overall strategy, may occur well in advance of any direct hostilities and last throughout any conflict. The potential for cyber aggression and the United States' readiness to confront this emerging threat to our defense networks is a timely topic for today's discussion and highlights the importance of Information Assurance.

In the last five months—since 1 October 1999—USCINCSPACE has focused efforts to "normalize and operationalize" CND across the DoD. A tremendous amount of effort is underway across the DoD to enhance Information Assurance.

USSPACECOM has a global responsibility for CND. As such, we have a global perspective of CND as it relates to IA. IA represents a set of measures aimed at protecting and defending information and information systems. CND is a key element of IA and must be carried out at all levels within our information systems. All CINCs, Services, and DoD Agencies that operate a DoD network are responsible for IA and subsequently responsible for defense of their networks. We know that a risk accepted by any one part of our network is a risk imposed on all parts of our network. Current initiatives such as the Defense-wide Information Assurance Program (DIAP) are critical, in our view, to provide the capabilities we need to protect and defend DoD networks in order to maintain Information Superiority. USCINCSPACE advocates increased resources, policies and practices to produce robust IA within the DoD.

However, there is a key difference between the IA and local CND responsibilities held by the CINCs', Services, Agencies and the responsibilities of USCINCSPACE. USCINCSPACE is responsible to look across all CINCs, Services, and Agency information systems within DoD to provide Joint Force Commanders and our National Command Authorities operational leadership for "Global Computer Network Defense." This view of global CND is more closely aligned with Defensive Information Operations (DIO) than that of IA. We agree with the importance to properly align responsibilities and authorities across the DoD for CND, and we will pursue this over the next several months as CND policies and directives are developed.

USCINCSPACE brings an operational perspective to plans, programs and policies across our DoD related to Information Assurance, especially those involving Computer Network Defense. As we move forward to build upon the existing DII towards a Global Information Grid (GIG), USSPACECOM will inject an operators view of what is required to effectively operate, protect and defend, our essential information networks. In concert with the essential nature of Information Superiority contained in Joint Vision 2010, we believe our defense information networks must be developed, operated and sustained just like any other “weapon system.” We advocate a layered information grid architecture to enable a defense in depth system that can be operated through established command and control methods.

“Protect and defend” includes a range of activities from DoD policy, to a collection of capabilities and procedures, to conducting defensive operations. When we conduct defensive operations, we will lead joint operations planning to develop and employ methods and capabilities to deter against cyber aggression. This approach is consistent within the Chairman’s joint instruction on Defensive Information Operations (DIO). This is important since the operational objective of any global computer network defense must be relevant to the Joint Force Commander in the conduct of overall mission operations.

Should our defense posture fail to deter cyber aggression, we will lead planning and operations to defeat a cyber adversary. All USCINCSPACE plans and operations will be conducted within the Joint Operations and Planning Execution System (JOPES).

Since USCINCSPACE assumed the DoD CND mission five months ago, we have led the DoD’s efforts to normalize and operationalize DoD networks to achieve Information Superiority. Here are a few highlights:

- USCINCSPACE established several initial priorities in order to protect and defend the information systems used everyday by our soldiers, sailors, airmen and marines as they carry out their duties around the world. Our first and foremost priority is to provide operational support to our Joint Force Commanders as they plan and execute missions around the globe. This is accomplished through CINC-level coordination and through the operational focus of Joint Task Force for Computer Network Defense, or JTF-CND. Concurrent with USCINCSPACE assumption of the DoD CND mission on 1 October, JTF-CND was resubordinated under USCINCSPACE as part of a major step to significantly enhance command and control for global CND operations across the DoD.
- Prior to the Y2K rollover, USCINCSPACE established Y2K as an operational priority. JTF-CND successfully executed a Contingency Plan to assess whether any Y2K-related event was malicious in nature. We learned a lot from this effort and today we are better able to meet emerging threats to our networks.
- USCINCSPACE also moved forward to transform existing processes related to the defense of our DoD networks. Across the DoD, we found that a tremendous amount of effort and hard work has gone into developing methods that reduce our vulnerabilities and communicate alerts to our forces worldwide. Now is the time to build upon these successes by applying this work to the way we normally conduct joint operations.
  - We intend to standardize and operationalize our DoD approach to Information Operations Conditions—or INFOCONs—in order to rapidly

synchronize required CND operations in support of our Joint Force Commanders.

  - Also, we will move to streamline lines of communication and operational reporting to enhance Joint Force Commanders and all DoD network operators appreciation for actions required to maintain Information Superiority.

- Another key USSPACECOM leadership effort involves injecting computer network defense operations into joint exercises. USCINCSPACE is committed to at least one major joint exercise per year to validate effective command and control of our global CND mission operations. This year's exercise is called APOLLO CND. It is in direct support of already planned USCINCPAC and USCINCTRANS concurrent exercises related to movement of material and personnel throughout the Pacific theater of operations. Joint exercises are an essential element of our efforts to validate joint concepts, tactics, techniques and procedures as we move forward to normalize and operationalize CND across the DoD. As our national security strategy evolves with respect to cyber aggression, we believe that joint exercises could also play an important role to demonstrate United States Information Superiority and leadership within the world.
- Finally, we have identified a whole range of important tasks that must be pursued in order to fulfill our goal to normalize and operationalize global CND operations. These tasks range from defining operational requirements, to shaping technology programs, to advocating for improved training, education, modeling and simulation. All of these efforts will center on increasing the operational readiness of our critical defense networks. We know that all of these supporting tasks are essential and will allow us to be able to operate, employ and sustain our critical

defense information networks just as we do other weapon systems. In this way, we will be able to maintain Information Superiority.

As an emerging threat, Information Assurance represents a major focus for USCINCSPACE as we lead the DoD towards normal and operational Computer Network Defense. It is an enormous challenge to operationalize the defensive efforts required to maintain United States Information Superiority. We are vigorously pursuing efforts to achieve effective global CND operations and we appreciate your continued support.