



SECURE THE NETWORK **Information Assurance** *"Secure The Data"*



As the military transforms to the information age, the linchpin of modern warfighting will be a **networked force** capable of **sharing assured information** and able to exchange a common battlespace picture. Protection of Department of Defense (DOD) information is imperative and the basis for trust when controlling forces in a fast moving combat environment. As such, government and industry play a vital role in equipping the modern warrior with systems that can meet the assured information requirements in the information age.

To meet the challenges of ensuring appropriate protection of information during transmission, processing and storage, the development and publication of DOD-level strategies are necessary to strengthen and synchronize DOD efforts to secure information. Key to this effort is the *National Military Strategy for Cyberspace Operations* (NMS-CO). The NMS-CO provides a comprehensive plan for DOD orchestration of national military strategic actions needed to operate and dominate in cyberspace. Additionally, DOD level guidance is required to address certification and accreditation; GIG policy; responsibilities and processes; IA controls; and critical infrastructure protection.

The joint community must establish methods and measures of effectiveness to identify and periodically assess our ability to protect DOD information. Acquisition strategies must be modified to improve network security through system assurance measures. Most DOD capabilities depend on systems developed in the commercial sector and these systems have high operational impact on the defense of our Nation and protecting critical infrastructure. Guidance and processes must be developed that actively ensure DOD systems are delivered with the highest level of inherent security. The Department of Defense must improve processes that provide shared situational awareness and monitor the performance, operational status and security of the GIG.

Government assistance is needed to:

1. **Standardize guidance** to strengthen and synchronize DOD efforts to protect data.
2. **Improve computer network defense** through training, doctrine, tactics, techniques, and procedures, and exercises.
3. **Define new encryption and data technologies** and procedures to enhance information integrity.
4. **Streamline the acquisition strategy** in order to keep pace with the technology advances available to our adversaries.
5. **Define acquisition processes** that ensure systems are received from reliable sources and systems come with security measures built-in.

Industry assistance is needed to:

1. **Develop computer network defense capabilities** that support automated approaches to protecting, monitoring, detecting, analyzing, and responding to unauthorized activities.
2. **Support a heterogeneous network defense tool** environment by building systems which interoperate among vendors.
3. **Design product suites** with inherent information assurance features.

Only through a combined effort by the government and the business world can we deliver the warfighter the fused, assured information required to gain battlefield success.

"We must stop building walls and digging moats as our primary means of protecting the network."
Nancy Brown, Vice Admiral, United States Navy, Director of C4 Systems, The Joint Staff