

**IAU Briefing Report
US Department of Defense
Directive 8581.1E**

On June 21, 2005, the United States Department of Defense (DoD) issued Directive 8581.1E regarding the information assurance policy for space systems used by the Department of Defense. This brief does not represent the entire DoD Directive, rather selective excerpts that the author views as prudent and pertinent to the reader along with commentary. Please see the directive in its entirety for more specific information.

4. POLICY It is DoD policy that:

4.1. All DoD-owned or controlled space systems shall meet the following system specific IA requirements regardless of mission assurance category (MAC) or classification:

4.1.2. IA shall be applied in a balanced manner by performing Information System Security Engineering (ISSE) as an integral part of the space system architecture and system engineering process to address all IA requirements in the intended operational environment.

4.1.3. The command links to DoD-owned or controlled space platforms shall be encrypted and authenticated on an end-to-end basis using National Security Agency (NSA)-approved cryptography.

4.1.4. Data generated onboard space platforms (e.g. telemetry and mission data) shall be end-to-end encrypted using NSA-approved cryptography.

4.1.10. DoD - owned or controlled space systems shall undergo IA certification and accreditation (C&A) in accordance with DoD Instruction 5200.40.

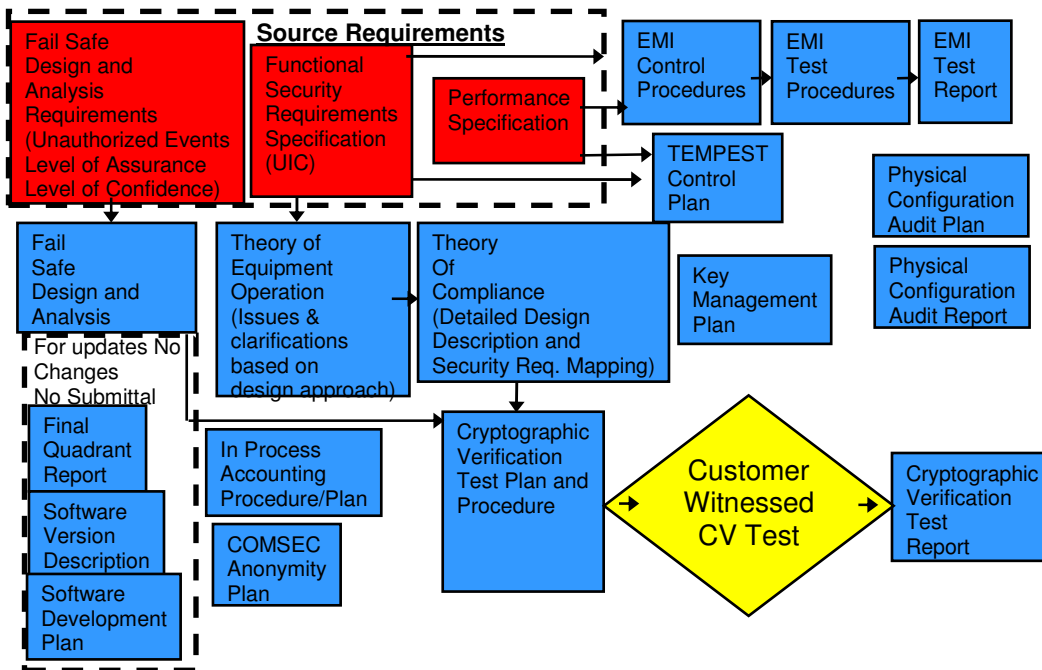
4.1.15. IA shall be a visible element of all space system investment portfolios. Data shall be collected to support reporting and IA management activities across the investment life cycle.

Why

“As we rely increasingly on space systems for trade, communications, imaging, intelligence gathering, military targeting and navigation, and other functions, the objectives of war planners can and will be achieved by attacking, compromising, or temporarily rendering inoperable a nation’s space assets”. - Military Space Systems: The Road Ahead by Matthew Hoey, February 27, 2006.

Accepting risks is no longer a viable alternative when it comes to significant space assets. With 9/11, with world has changed and risk must be mitigated, through multiple layers of defense that is not add-on, but rather integrated into everything we do. With regard to a space-based vehicle, information assurance must be maintained throughout its operations, from deployment to de-orbit. This means that the system must be certified and accredited.

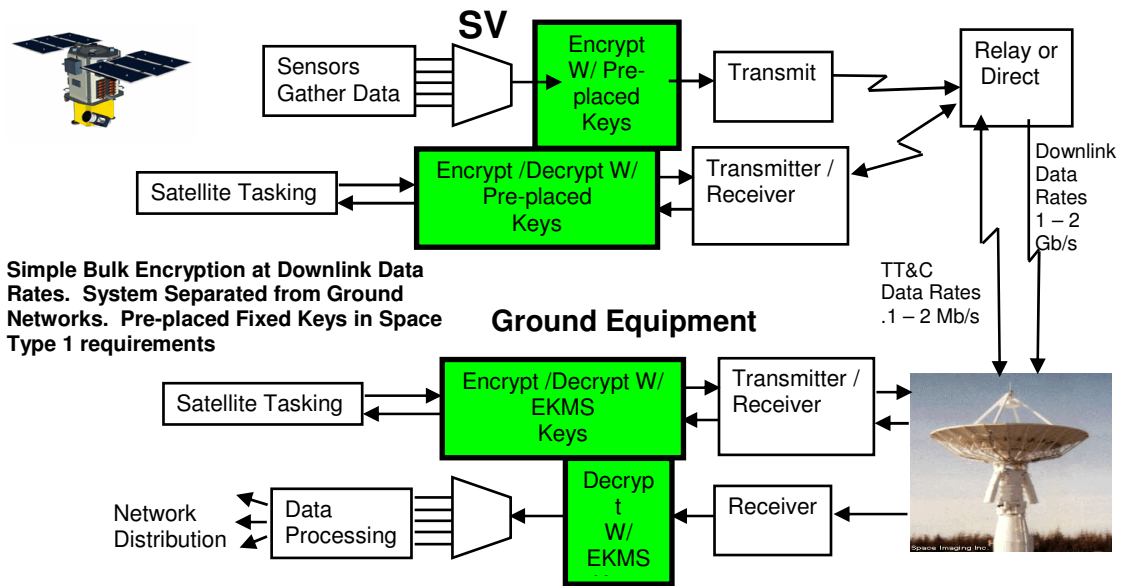
The following is the certification process for space-based vehicles:



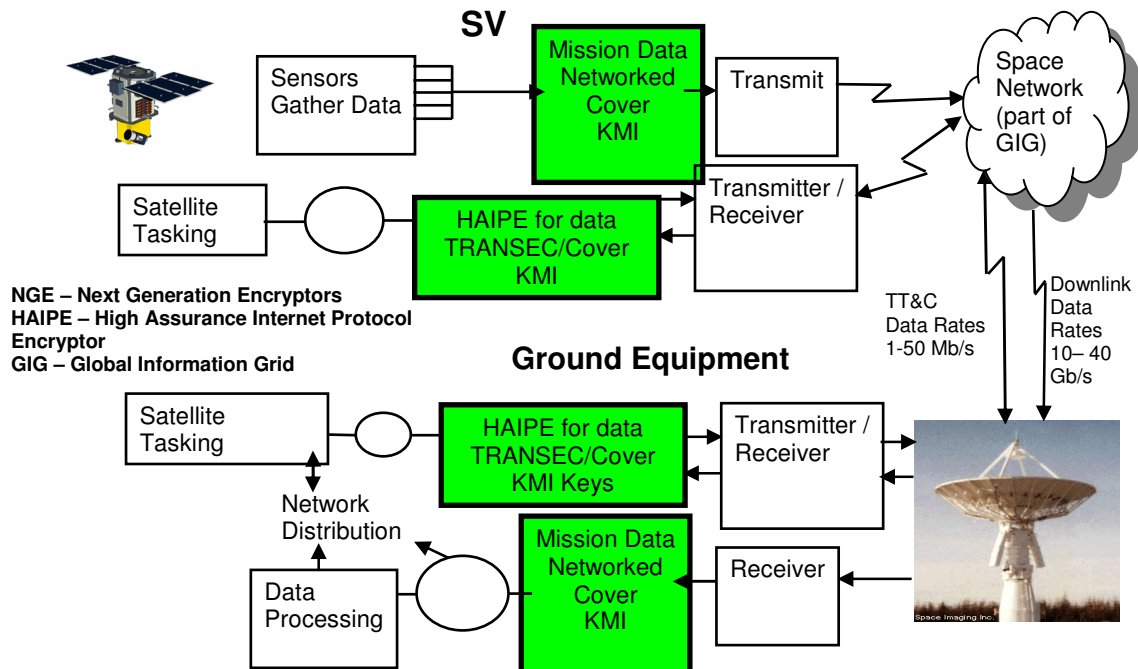
With regard to the certification process, plan for at least a one year schedule. The use of an experienced Information Assurance expert may significantly reduce both the risk and the cost of approval.

Remember Mission Success=Mission Secured

Current Space Encryption Model:



Future Space Encryption Model:



For more information regarding DoD Directive 8581-1E, please see the following link: <http://iase.disa.mil/dodd-8581-1e-faq.doc>