

## Information Assurance in the Next Generation Small Satellites May Become the Law!

**Gene Katz**  
**General Dynamics C4 Systems**  
**Information Assurance Division, Business Development**  
**8220 East Roosevelt Street, Scottsdale AZ 85257; (480) 441-6280**  
**gene.katz@gdc4s.com**

**ABSTRACT:** Micro SATs and Mini SATs utility/ mission capabilities continue to advance well beyond academic projects and technology demonstrators. Sophisticated payloads with complex mission data are becoming the program drivers, complimented with the concepts of satellite swarms and low cost launch vehicles. All this is evidence for a strong future in the use of this technology. The bad news is that this growing success will make it a target for sinister exploitation. The un-thinkable happened in September 2001 when commercial aviation assets were hijacked and turned into weapons of mass destruction. Can this happen to our SPACE assets? This paper explores the implications of necessary security architectures applicable to satellite technology. An introduction to information assurance requirements is presented including the NSA certification process details. If it is a classified mission, these requirements are required by law. If it is in SPACE, these requirements may be our only defense in preventing a space Pearl Harbor. Cost effectiveness is achieved by taking information assurance issues upfront and designing them in as apposed to adding later. This paper will introduce the latest information assurance issues and direct readers to numerous web sites for more details and guidance on requirements, best practice, and the governing laws.

### INTRODUCTION

From the Congressional Transcripts of the Senate Armed Services Subcommittee on Strategic Forces FY2007 Budget: Military Space Programs, the honorable Ronald Sega, Undersecretary of the Air Force and DoD executive agent for space stated:

“ ... small satellites and a subset of those are TacSats, will be part of our future going forward.”

Offered as part of the “back to basics” approach the DoD and the Air Force is taking to get space acquisitions back on track includes making use of small satellite technology as quicker and cheaper where appropriate. It doesn’t get any better than that for creating new market opportunities other than declaring it law. But, what comes with this declaration is the burden of attention, or better said, becoming a target for someone or some government alternative agenda. You might still feel that space is hard to get to and access is very expensive. These two attributes historically have been our sense of security. Taylor Dinerman,

author and journalist wrote for The Space Review, March 13, 2006:

“The biggest space targets for terrorists are here on earth. Ground control stations, industrial sites, and even critical individuals are all possible targets for terrorists who want to disrupt satellite operations.”

Matthew Hoey wrote earlier in the year, February 27, 2006; Military Space Systems: the road ahead

“The combination of affordable, short-notice launch capabilities with small satellite technology has the potential to revolutionize the space industry, especially military space systems.”

With all this publicity, being in the news and building expectations that this technology is ready for prime time suggests we had better start thinking about the unthinkable. That is to say, how should we design our small satellite systems such that they can never be used against us or in ways that were never intended. That is what Information Assurance is all about.

## INFORMATION ASSURANCE HAS ITS OWN VOCABULARY

Anytime we begin the study of a new subject it is inevitable that begin with unique vocabulary. IA is no exception. The Holy Grail is shown below in Table 1.

Table 1 - IA unique vocabulary

Attribute	Definition
Access control	Process of allowing or disallowing access based on many criteria, including but not limited to successful authentication. Access control protects against unauthorized use of a network or networked resource.
Availability	Methods to maintain availability prevent the denial of service through degradation of network services.
Authentication	Establishment of the identity of an entity (either a user or a computer system). Authentication in this document also includes non-repudiation.
Non-repudiation	Non-repudiation is the provision that an entity sending or receiving a communication cannot later deny sending or receiving that communication.
Confidentiality	Methods to maintain confidentiality protect information from being disclosed to unauthorized entities.
Data integrity	Methods to maintain data integrity detect (but do not necessarily prevent) the unauthorized modification or deletion of data.
Traffic flow integrity	Methods to maintain traffic flow integrity prevent the collection of sensitive information about the network through observation of network traffic characteristics. This includes gaining information about the network based on when traffic does or does not flow or based on packet headers being sent to, from, or within the network.

These seven definitions are the fundamental basis for all information security principles. The trick is the application of security policies, enforcement of those policies and the use of various technologies for defense in depth. Defense in depth is mandated by DoD as the main IA implementation strategy to be used to protect national security systems and information. This approach emphasizes the construction of successive layers of defense to protect against attacks. NSA is responsible for providing guidance regarding the appropriate combination and implementation of government and commercial IA-related products in national security systems.

## IA IS ABOUT HOW PARANOID, NOT IF YOU ARE PARANOID

Try a little experiment sometime. While in front of your car go up to a perfect stranger and give them the keys to your car, then just walk away. How do you feel? That feeling is a certain level of paranoia. If you actually refuse to do it, you are qualified to study IA. What keeps you up at night? Mission details, technical challenges, schedules, budgets, people? Well, it should be whether you are paranoid enough.

## IF THE GOVERNMENT WILL OWN OR CONTROL SPACE SYSTEMS, THEN IA IS THE LAW.

Department of Defense DIRECTIVE 8581.1 E is the Information Assurance (IA) Policy for Space Systems used by the Department of Defense. Section 4.1 clearly states:

“4.1 All DoD-owned or controlled space systems shall meet the following systems 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.”

## IT IS JUST A MICRO SATELITE.

As the utility value of Small Satellite technology grows so does the awareness of them. We tend to view the technology as an alternative to traditional space missions that provide complimentary utility as apposed to disruptive technology. Successful implementation of lower cost access to space and responsive space processes will fuel the much anticipated exploitation of Small Satellites. However, it is not just the out of the box thinking on how this technology can be used to solve complex mission scenarios, but rather the fact that they are there and therefore, others will try to exploit them for their own agenda in ways the originators never dreamed of. Information Assurance designed in will be the only defense against such exploitations. It is the intention of IA designers to make systems secure end to end and as transparent to the user as possible. The technical mission challenges and details tend to over shadow the particulars of IA and budget dollars are too thin to support what may be perceived as non-value added. Again, careful

consideration to the total lifecycle costs must be made to determine the level of risk to accept verses investing in IA risk reduction. Then again, how do you value the risk of highjacked assets exploited as weapons of mass destruction?

Bottom line is that the world has changed significantly in that each of us can no longer just accept the risk. Therefore, mitigating the risk requires the best possible designs that offer a multi-layered defense that is maintained throughout the development and mission operations through de-orbit. This means that the system must be certified and accredited.

MORE 8581.1 E

“4.1.10 DoD – owned or controlled space systems shall undergo IA certification and accreditation (C&A) in accordance with DoD Instructions 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.”

#### CERTIFICATION PROCESS

Certification process is a multi- step process with many deliverables that all lead up to a Customer witnessed CV test. DoD 5200.40 is called the “DoD Information Technology Security Certification and Accreditation (C & A) Process (DITSCAP)” December 1997, The domains covered include:

- Fail safe design and analysis
- Functional Security requirements
- Performance Specifications
- EMI Control Procedures, tests, reports
- TEMPEST Control Plan
- Physical Configuration Plans
- Audit Reports
- Key Management Plan
- Final Quadrant Report
- Software Version Description
- Software Development Plan
- In Process Accounting Procedure/Plan
- COMSEC Anonymity Plan
- Cryptographic Verification Test Plan
- Customer Witnessed CV Test
- Cryptographic Verification Test report.

Plan for at least a one year schedule effect and is spread throughout the development lifecycle. Use

the help of an IA expert that has done this before to reduce the risk and cost of approval in a timely fashion.

#### IT IS A LICENSE TO LEARN

At this point it is all about learning what Information Assurance is and how to do it. The subject matter is not standard curriculum in our systems engineering classes (but should be). So, where do you go to get more guidance? The Systems Engineering level is a good place to begin. Numerous Web sites are available from agencies, industry, and educational institutions, should you choose to go it alone. I offer the following as a starting point:

Information Assurance Technical Framework, Version 3.1 September 2002  
<http://www.iatf.net/>

Information Security Configuration Guides  
<http://www.nsa.gov/snac/>

DoD Instructions 5200.40 DITSCAP  
<http://iase.disa.mil/ditscap/DITSCAP.html>

DoD Directive 8500.1  
[http://www.dtic.mil/whs/directives/corres/pdf/d85001\\_102402/d85001p.pdf#search='DoD%208500.1](http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf#search='DoD%208500.1)

DoD Directive 8581.1 E  
<http://www.dtic.mil/whs/directives/corres/rtf/d85811x.rtf>

FAQ about 8581.1 E  
<http://iase.disa.mil/dodd-8581-1e-faq.doc>

Centers of Academic Excellence in Information Assurance Education  
<http://www.nsa.gov/ia/academia/caeiae.cfm>

Information Security Management Handbook 4<sup>th</sup> edition, Harold F. Tipton and Micki Krause Auerbach publications, ISBN 1-8493-9829-0

IP-in-Space Security Handbook, September 2001  
<http://ipinspace.gsfc.nasa.gov/documents/>

Satellite Encryption, John Vacca  
Academic Press, ISBN: 0-12-710011-3

## CONCLUSION

**Now is the opportunity to do it securely. The Small Satellite assets will definitely find their place in our government inventory in new and meaningful missions. We need to embrace the principles of Information Assurance in Small Satellite system architectures because of the laws but more importantly, it is the right thing to do. The focus is on the mission success where it needs to be. Our new world order requires us to bake in the security of the system as well as to insure that our system can never be used against us in any capacity. Think the unthinkable and how to prevent it from ever happening and then it won't. Information Assurance is not new, however it is ever expanding in our Information Age. Seek out subject experts early. Embrace the fact that Mission Success = Mission Secured.**