# Systems Engineering Area (DRAFT UPDATE)

## Security Working Group

|  |  |
| --- | --- |
| **Title of Group** | **1.2 Security Working Group** |
| **Chair** | **Howard Weiss/NASA** |
| **Area Director** | **Peter Shames/NASA** |
| **Mailing List** | [**sea-sec@mailman.ccsds.org**](mailto:sea-sec@mailman.ccsds.org) |

### Rationale

CCSDS develops communications and mission operation standards that support inter and intra agency operations and cross support. CCSDS standards include elements of flight and ground systems that are developed and operated by different agencies and organizations.

Given that ubiquitous network connectivity among principal investigators and mission operations has become the norm, mission operations have become more dangerous than in the past when operations were carried out over closed, mission-only networks. The security risks to both spacecraft and ground systems have increased to the point where CCSDS must adopt existing or develop (as necessary) Information Security standards in order to protect both flight and ground mission critical resources and protect sensitive mission information.

Mission planners must perform mission threat analyses to better understand the threats that they should plan to counter via security requirements. Mission planners must also design security into their systems from the outset to ensure that security does not obscure mission requirements and vice-versa. CCSDS must promote secure interoperability for space missions. CCSDS also requires Information Security standards as part of, or as an accompaniment to its communications and mission operations standards.

In order to help the mission planner successfully design “in” security the CCSDS Security Working Group will provide “tools” such as security standards, guides, and architectures which must be identified, maintained, and updated to ensure relevancy with current threats identified by CCSDS as well as other sources.

### Goals

The goals of the Security Working Group are to:

1. provide advice and guidance on information security to all CCSDS activities and working groups;
2. identify data protection, information assurance, and information security issues across the full spectrum of CCSDS activities and provide solutions;
3. adopt or develop (as necessary) interoperable security standards for CCSDS and CCSDS cross support infrastructure (e.g., authentication, encryption, integrity, key management, key distribution);
4. formulate courses of actions to incorporate security policies, security services, and security mechanisms into CCSDS work items across all Working Groups;
5. hold working meetings with other Working Groups to develop agreed approaches and formulate the plans for integrating them into the work of these other Working Groups
6. develop and maintain a CCSDS security architecture;
7. develop and maintain an Information Security threat statement for CCSDS which is periodically reviewed in order to remain relevant with the evolving threat environment against space missions;
8. develop reference implementations and perform interoperability testing.

In addition, the Security Working Group shall develop and maintain specific guides (Green Books) and best practice documents (Magenta Books) such as:

1. an information security guide for mission planners;
2. a policy framework for developing trust agreements, rules for operational engagement, ensuring security compliance of legacy systems, and standard, secure interfaces between systems and across security domains;
3. to investigate the possibilities of integrating relevant existing and arising standards (e.g., the Common Criteria (ISO 15408)) into the development of mission security requirements and other documents;
4. a key management guide to introduce the concept of key management and potential alternatives available for missions;
5. a description of security guidelines for implementation and testing;
6. a guide to standardized cryptographic algorithms;

### Schedule and Deliverables

| **Date** | **Milestone** |
| --- | --- |
| 30 May 2003 | WG established. |
| January 2005 | Deliver revised Security Green Book. |
| February 2005 | Circulate Security Architecture White Book to working group for comments. Circulate Threat Document for final WG review. |
| April 2005 | Security WG meeting in Athens. Review final comments on Threat Document. Review Security Architecture White Book. |
| May 2005 | Publish completed Threat Document as a Green Book. Issue Security Architecture as Red-1. Develop an encryption standard trade study proposal. |
| July 2005 | Develop an authentication standard trade study proposal. |
| September 2005 | Review RIDS on Security Architecture Red-1 at Sec WG meeting. |
| October 2005 | Issue draft Policy Guidelines document based on NIST document. |
| December 2005 | Mission Planners Guideline – maybe based on tailored version of Common Criteria. |
| January 2006 | Issue encryption Red-1. |
| February 2006 | Issue authentication Red-1. |

### Risk Management Strategy

#### Technical Risks

Security is a “different” and often obtuse part of CCSDS’ work and is often treated as an “outsider.” It is not “mainstream” CCSDS work nor is it “traditional” CCSDS work. In the past, it has been met with resistance. However there is now general acceptance of the need for security services for civilian space missions and interactions with other working groups are increasing. Working group resources have increased but are still not entirely adequate.

#### Management Risks

Unavailability of resources will delay achievement of milestones. Fallback option would be to reschedule the milestones.

Identification of specific security guidelines may result in additional work items being agreed upon with other working groups.

### Resource Requirements

|  |  |
| --- | --- |
| Lead Agency | NASA |
| Participating Agencies | NASA |
| ESA |
| CNES |
| UK Space Agency  DLR  ASI  CNSA (CAST)  (core agencies who have commitment to document and action item production) |