Example Security Sections for non-Blue/Magenta CCSDS Documents

1. CCSDS 130.0-G-4 – Overview of Space Communications Protocols:
   1. This document introduces space communications protocols, the features of space communications protocols, and examples of protocol configurations. But in its latest revision, it only casually mentions security services (e.g., the last paragraph of Section 2.1 which acknowledges the need for security and calls out various CCSDS security-related documents, Section 2.2.3 mentions SDLS security services available at the link layer). It does not discuss the use of IPSec (despite discussing IP) or BPSec (despite discussing DTN). Personal observation: not only does this document need a security section, but it needs security to be strongly intertwined in each of the sections. The protocol diagrams in section 4 totally ignore security. It does not reference the CCSDS Security Threat document nor does it mention threat/risk.
   2. A possible ‘Section 5 Security’ for this document might look like:
      1. Security is of great concern to space missions. The threats to space missions have increased greatly over the years particularly regarding spacecraft commanding and data integrity and confidentiality. It is recommended that security mechanisms and services be applied to one or more protocol layers as are illustrated in Figure 2-1. (NB – this diagram should be revised to also include BPSec, IPSec, and SDLS which are currently not shown).
      2. Missions must consider the potential threats against their systems both on the ground and in space. They must architect their systems with security built in from the start and not bolted on as an afterthought. As the mission architecture develops, they mission planners must consider the threats against each protocol layer and what mechanisms, taken from CCSDS recommendations, employed to counter the threats. Missions must ensure that spacecraft commanding is secure and data transmission to and from space is provided confidentiality and privacy from source to destination.
      3. Secure spacecraft commanding is critical to the overall security of a mission. Commands transmitted to a spacecraft should, at a minimum, be authenticated prior to acceptance and execution by the spacecraft. For critical missions, the commanding might also employ confidentiality of the commands using authenticated encryption techniques to ensure that not only are the commands authenticated but also kept private from being viewed by those who do not need to see the command format or content.
      4. CCSDS has published many security-related documents, including The Application of CCSDS Protocols to Secure Systems (reference [37]), Security Architecture for Space Data Systems (reference [53]), CCSDS Cryptographic Algorithms (reference [54]), the Space Data Link Security (SDLS) protocol, and the SDLS Extended Procedures (references [43] and [58]), to provide guidance to missions that wish to use the CCSDS space communications protocols for spacecraft control and data handling but also require a level of security or data protection.
2. CCSDS 706.2-G-2 – Voice Communications:
   1. This document already contains a ‘security’ section (section 3.2.3.3) which acknowledges the need for voice security for privacy (e.g., medical) as well as critical operations. But while a good start, this section only pays lip-service to voice security. It mentions some security techniques but does not specify or recommend anything.
   2. A possible expanded security section for this document might look like this:
      1. Security for the voice segment of space missions, both on the ground and in space for crewed missions, is vital.
      2. For the ground segment, voice communications that extend beyond a single control center must be considered to be at risk for eavesdropping and jamming which could threaten personal privacy or the life of a mission. Such communications should employ encryption to ensure confidentiality and privacy. Secure voice may be able to employ off-the-shelf voice security systems as are currently used in Voice-Over-IP (VoIP), digital first responder radios, and mobile phone systems. For national security systems, voice security systems may be obtained from the nation’s agency responsible for secure communications.
      3. For the space segment, with a crewed mission, astronaut medical data must be protected and remain confidential in accordance with national laws. Critical technical aspects of the mission must also be confidential to minimize or reduce risk to the overall mission. As is the case for the ground segment, VoIP confidentiality techniques can be used to provide secure voice communications.
      4. The mission should be designed with voice security from the outset to ensure that a compromise does not occur.
3. CCSDS 706.1-G-2 – Motion Imagery and Applications:
   1. This document is an excellent overview of digital video technology and its application for space. Section 3 delineates the various motion imagery parameters such as resolution, compression, chroma sampling, audio, and aspect ratio. However, for the most part, security is absent. A security section should be added integral to the document as opposed to an Annex. Security is mentioned at the end of Section 4 (integrating video applications to other standards).
   2. A possible security section for this document might look like:
      1. The Motion Imagery and Applications Working Group will analyze, test, prototype and report on recommendations and best practices for digital video and motion imagery utilizing existing CCSDS and industry standards and protocols and establish recommendations for applications of digital video and motion imagery to include quality of service, IP, and broadcast protocols, including multicast and unicast, security, and privacy. *(borrowed from Section 4)*
      2. From a security perspective, motion imagery must take into consideration the privacy and confidentiality of both 2-way video (e.g., video conferencing) as well as the downlink and transmission of imagery files in all cases other than public ‘press conferences.’ The imagery systems should be integrated as a secure flow over secure data networks and on the ground, afforded authentication, integrity, and access controls.
      3. Application of non-CCSDS video standards – e.g., DVB scrambling, DRM, HTML5 video encrypted media extensions, high-bandwidth digital content protection (HDCP), Cable TV distribution encryption (DOCSIS Data-over-Cable Security Specification), encrypted multicast, etc to provide imagery security mechanisms?
4. CCSDS 130.12-G-2 – CCSDS Protocols over DVB-S2:
   1. This is a newly published document (June 2023) that does not have a single mention of security. Yet, DBV has security specifications available discussing ‘scrambling’ (encryption) and security processors, but these are not referenced. This document should include references to the DVB security documents and should have an integrated security section, maybe in Section 4 (Implementation at the interface between CCSDS protocols and DVB-S2). Not being a DVB or link layer person, here is a feeble attempt at what a security section might look like:
      1. Section 4.4 Secure Use of DVB-S2 in CCSDS: Security of data transmitted via DVB-S2 is of paramount importance for CCSDS space missions. The DVB Security Processor, which is a separate processor manufactured to much higher security requirements than the main CPU, carries out security functions such as decryption, stores secure information such as keys. The DVB SimulCrypt and Scrambling Algorithm version 3 (ETSI TS 100 289 V1.2.1), which uses the CCSDS recommended AES encryption algorithm, should be integrated, and used for CCSDS missions.