1. Presentation Title:

The State of CryptoLib – The Open-Source Satellite Cryptography Library

2. Presenter:

\* Enter Name, Title, Organization, Email, and Phone number

D. Cody Cutright, Systems Engineer

TMC Technologies, NASA IV&V

cody.cutright@tmctechnologies.com

(304) 516-2145

3. Short Biography of Presenter: (100-200 Words)

Cody is a member of the NASA's Independent Verification & Validation JSTAR Team in Fairmont, WV. His primary focuses are integration of satellite ground station software into digital twins, CCSDS protocol implementation and configuration, and furthering development of open-source cryptography . Cody is a lead developer on the open-source cryptography library - CryptoLib - which aims to be a compliant implementation of the CCSDS Space Data Link System protocol. He possesses a Master's in Electrical Engineering from West Virginia University, and a Bachelor's of Computer Science & Mathematics from West Virginia Wesleyan College. In his spare time he enjoys hiking in excess of 2,000 miles at a time, and serving as a Firefighter / Paramedic.

4. Other Authors:

\* Enter Name, Title, Organization, Email, and Phone number

\* Robert J. Brown, Systems Engineer, TMC Technologies, NASA IV&V, Robert.Brown@tmctechnologies.com

\*John P. Lucas, Systems Engineer & JSTAR Deputy Lead, NASA IV&V, John.P.Lucas@nasa.gov

\*Justin R. Morris, Computer Engineer & JSTAR Lead, NASA IV&V, Justin.R.Morris@nasa.gov

\* Scott A. Zemerick, Chief Engineer, TMC Technologies, NASA IV&V, Scott.Zemerick@tmctechnologies.com

5. Point-of-Contact if other than Presenter:

6. Keywords: (short list of focus areas addressed in your presentation)

- open-source encryption, cybersecurity, resilience

7. Has this abstract been approved by your organization? \*

8. If accepted, will you allow your presentation to be included on the GSAW website?

Yes

9. Abstract: (200 Words to Two Pages)

What state would the world be in if all internet traffic was unencrypted? Imagine an alternate universe where you can plug a packet sniffing device into your home internet and capture the web traffic of the entire world. It seems obvious that this scenario is less than desirable. If we would not allow this for the internet, why would we allow this in the space domain? With the advent of open-source ground stations, commercial off the shelf hardware, and ground stations as a service, the barrier to entry for space communications is rapidly lowering. New players enter the space realm every day, and the presence of tools to allow apprentice evildoers the ability to exploit satellite communications is on the horizon. Not only are legacy missions at risk, but future missions are as well - particularly lower budget missions with more stringent size, weight, and power constraints that may find it difficult to utilize hardware-based encryption solutions.

In terms of Civilian Aerospace, NASA Standard 1006 directs that missions "shall protect the command stack with encryption that meets or exceeds Federal Information Processing Standards (FIPS) 140". Fortunately, the Consultative Committee for Space Data Systems (CCSDS) has published an international standard on Space Data Link Security. The combination of these two forces has resulted in CryptoLib - an open-source, C-based, encryption library that aims to be CCSDS SDLS compliant.

CryptoLib is designed to support smaller missions on a tight budget that may be subject to the more stringent command link encryption requirements. Additionally, CryptoLib serves as an underpinning in JPL's Key Management & Cryptography (KMC) suite and is also designed to function as a 'drop-in' for smaller missions. CryptoLib is in active development and currently provides Telecommand (TC), Telemetry (TM), and Advanced Orbiting Systems (AOS) encryption and decryption capabilities with a variety of encryption and authentication schemes. This presentation will report the latest features, current status, and future plans for CryptoLib.

\* Aerospace Corporation employees are required to have abstracts and presentations cleared through the Office of Technical Relations (OTR) process

GSAW Plenary Abstract

When completed, submit to gsaw@aero.org Revised 8/10/2023

 OTR 2023-01064