Paper ID: 64255
oral

IAF SYMPOSIUM ON SPACE SECURITY (E9)
Cyber-based security threats to space missions: establishing the legal, institutional and collaborative framework to counteract them (2)

Author: Mr. PJ Blount
University of Luxembourg, Luxembourg , pjblount@gmail.com

GETTING NIST-Y WITH IT: UNITED STATES LAW, POLICY, AND STANDARDS FOR CYBERSECURE SPACE OPERATIONS

Abstract

The United States has, arguably, been a leader in the area of cybersecurity for space operations. Even before the release of Space Policy Directive 5 on cyber secure space operations, the Committee on National Security Systems had developed a Space Platform Overlay that addressed cybersecurity for national security space operations using the NIST 8000-53 control list. Today, the United States Space Force's IA-Pre has adopted a similar approach for commercial satcom partners bidding on military contracts.

Despite the lead that the United States is taking in the area, this is not a complete project nor a simple one. The IA-Pre framework designates hundreds of controls to be implemented on satcom solutions before they can be considered for a contract. The complexity can be quite burdensome for small companies, and the adopted frameworks may be to rigid for non-national security payloads. This paper will survey the landscape of cybersecurity for space assets from a US perspective through the lens of law, policy, and standards in order to identify gaps and propose a more general framework for general space actors.

This paper will proceed by investigating in turn, the legal landscape for cybersecurity, the policy landscape with an emphasis on SPD-5, and the standards landscape with an emphasis on the NIST Risk Management Framework. It will conclude with recommendations on how further capacity can be built in this area, not just within the US, but for global operators.