Paper ID: 67693
oral

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

Author: Mrs. Rose Mustain
NASA, United States, e.r.mustain@nasa.gov

Mrs. Svetlana Hanson
NASA, United States, svetlana.hanson.dtm@gmail.com
Ms. Rosa Sosa
NASA, United States, rosa.sosa@nasa.gov

GATEWAY IMPLEMENTATION OF CYBERSECURITY REQUIREMENTS

Abstract

Cyber threats are a constant present-day reality for any type of business – Space exploration is not excluded from these threats either. The Gateway Program is one of NASA's latest initiatives that extend space exploration beyond low earth orbit. Gateway allows for NASA to prove technologies and mature systems necessary to live and work on another celestial body before embarking on multi-year missions to Mars. The Gateway is a small, human-tended space station in orbit around the Moon. With the increased autonomy, distance and criticality of systems, cybersecurity is one of the critical subsystems that touches and integrates with most if not all subsystems of the Gateway. Building a gateway to the lunar orbit is no simple task. In this presentation, we outline an approach that the Gateway team adopted in creating a cyber safe and robust vehicle to support operations and assure protection of the critical functions. Gateway Program is required to implement National Institute of Standards and Technology (NIST) guidelines to adhere to the Federal Information Security Modernization Act (FISMA). NIST provides a framework for managing and controlling cybersecurity risks by defining cybersecurity controls and methodologies for implementation. The NIST framework is based upon the system, data within the system, integrations with external systems, and risk assessments to determine impacts for each of those systems. The goals and objectives are to identify appropriate security controls that fulfill and map to the NIST 800-53 framework. The implementation process involves developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. NIST Security controls are interpreted and defined within the Gateway vehicle requirements subsystems specifications. This paper details the approach, implementation, and challenges faced during the development and design phases to address cyber threats during the Gateway vehicle operations.