System Documentation

1 System Description

1.1 Purpose and Capabilities

1.2 System Components

1.2.1 Software Components

1.2.2 Third-Party Components/Services

1.3 Stakeholders

1.4 Operational Environment

2 Data Flow Analysis

2.1 Data Identification

2.1.1 Types of Data Processed

2.1.2 Data Classification

2.2 Data Flow Diagrams (DFDs)

2.2.1 Level 0 (Context Diagram)

High-level representation of external interactions with ground control, cloud storage, and third-party services.

2.2.2 Level 1 DFDs

Detailed flow between onboard sensors, processors, storage, and communication systems.

3 Security Categorization

3.1 Reference Standards

- FIPS 199: Security categorization for federal systems.

- NIST SP 800-60: Mapping security categories to information types.

3.2 Impact Levels (Confidentiality, Integrity, Availability)

3.3 Overall Categorization

3.4 Justification

4 Risk Management & Compliance

Alignment with Risk Management Framework (RMF) per NIST SP 800-37. Categorization informs security control selection (NIST SP 800-53). Ongoing assessment and mitigation per FIPS 200 minimum security controls.

5 Deliverables

- **System Description Document**: A comprehensive report covering all aspects outlined in Section 1.

- **Data Flow Diagrams**: Level 0 and Level 1 DFDs with annotations.

- **Security Categorization Whitepaper**: Detailed analysis and justification of the security categorization. See section 4.5 of NIST Special Publication 800-60 Volume I Rev. 1.