Data Protection Plan Template

1. INTRODUCTION

1.1 Objective
This document provides a framework from which a NOAA licensee may develop a Data Protection Plan tailored to the relevant license for all privately-operated, including commercial, U.S. remote sensing satellite systems. A licensee is required to submit a Data Protection Plan per 15 CFR, Section 960.11(b)(13).

1.2 Scope
Data Protection Plan (DPP) refers to the licensee’s plan to protect commands, data and information through the entire cycle of tasking, operations, processing, archiving and dissemination. At a minimum, this includes appropriate protection of communications links and/or delivery methods for tasking of the satellite, downlinking of data to a ground station (including relay stations), and delivery of data from the satellite to the licensee’s central data storage facilities.

The template will minimize documentation of information contained within the relevant commercial remote sensing license and license application, or information that is not relevant to the task of reviewing of the licensee’s data protection strategy.

The request for certain information within the template is restricted to commercial remote sensing systems of a specific class. Determination of class is the prerogative of the licensing authority, and class descriptions as provided in the appendix are for reference only.

1.3 Data Protection Strategy
This section describes high level elements of the licensee’s data protection strategy.

1.3.1 Summary
Provide a brief description of the data protection strategy that encompasses the remote sensing system including the space segment, ground segment and modes of communication.

1.3.2 Data Protection Diagram
Provide a diagram that describes the flow of information between elements of the remote sensing system and identify protection mechanisms, such as encryption, which prevent unauthorized access. Identify mechanisms that protect data moving between physical elements of the remote sensing system and, if applicable, mechanisms that protect data at rest.

2. SPACE SEGMENT
The space segment includes the satellite(s) which are regulated by the NOAA commercial remote sensing license associated with this DPP.
2.1 Space Segment Description

2.1.1 Orbital Information
Describe the nominal orbital parameters for each space vehicle, including altitude and inclination.

2.1.2 On-Board Propulsion
Describe the maximum $\Delta V$ and maximum acceleration for the space vehicle(s).

2.1.3 Sensor(s)
Briefly describe each sensor having a remote sensing capability that is regulated by the licensing authority.

2.2 Communications

2.2.1 Communications Links
Identify all communications links between elements of the space segment and ground segment including:

- **Link ID**: Descriptive name or similar classifier for the link.
- **Direction**: Identify whether the link is an uplink, downlink, crosslink or a composite.
- **Frequency**: Identify the frequency or the wavelength over which the link operates.
- **Data**: Identify the type or types of data which are transferred over the communications link.
- **Encryption**: Identify whether the link is protected with encryption or if it is unsecured.

2.2.3 Link Characteristics [Class 3 Systems Only]
For each communication link, describe the physical characteristics of the link including the type(s) of data passed over the link as well as the frequency, modulation scheme, data rates, transmit antenna gain patterns and radiated power levels. Discriminate between telemetry or engineering data, satellite command and control data, and remote sensing data.

3. GROUND SEGMENT

The ground segment includes all ground infrastructure directly associated with command, control and mission data which are regulated by the NOAA commercial remote sensing license associated with this DPP.

3.1 Ground Segment Locations

3.1.1 Ground Segment Locations
Identify all ground segment facilities that handle protected data:

- **Facility ID**: Descriptive name or similar classifier for the facility.
- **Location**: Descriptive location such as an address which includes the nation in which the facility resides if applicable.
- **Coordinates**: Identify the latitude and longitude of the facility, or otherwise identify the facility as mobile if applicable.
Function  Identify the function(s) of the facility including any ability to encrypt and send commands to the space segment or decrypt protected communications links.
Ownership  Identify the owner and/or operator of the facility and identify any foreign interests.
Contact  Provide a point of contact for the facility.

4. SECURITY PLAN

4.1 Physical Security
Physical security measures may include some or all of the following: fences, locks, alarms, video monitoring, and guards which prevent or detect physical access to elements of the Ground Segment. Where third party systems and facilities are used (e.g., public cloud infrastructure providers), tailor the level of detail as appropriate and relevant.

4.2.1 General Security Measures [Class 2 and Class 3 Systems Only]
Identify specific physical security measures and protocols implemented to prevent unauthorized access to each ground segment location. Identify security measures which monitor and control the movement of personnel into, out of, and within the location(s).

4.2.2 Cryptographic Hardware [Class 2 and Class 3 Systems Only]
Identify additional physical security measures and protocols, if any, implemented to prevent unauthorized access which could compromise the cryptographic protections identified in this DPP.

4.2.3 Remote Sensing Data [Class 3 Systems Only]
Identify additional physical security measures and protocols, if any, implemented to prevent unauthorized physical access to stored remote sensing data.

4.2.4 Personnel [Class 2 and Class 3 Systems Only]
Identify specific measures implemented to vet personnel with access to protected data and space vehicle command and control.

4.3 Network Security

4.3.1 Command and Control [Class 2 and Class 3 Systems Only]
Identify network security measures which protect access to space segment command and control functionality. Specify how access to satellite command and control functions will be protected and audited.

4.3.2 Distribution [Class 3 Systems Only]
Identify network security measures which protect access to sensitive data during transmission to approved customers.

4.3.3 Storage [Class 3 Systems Only]
Identify network security measures which protect access to sensitive remote sensing data or encryption keys while stored on networked systems.
4.4 Cryptographic Security

4.4.1 Encryption [Class 2 and Class 3 Systems Only]
For each encrypted communication link identified in Section 2.2.1 Communications Links, describe the method of encryption including cipher(s), mode(s) of operation, and authentication schemes.

4.4.2 Key Management [Class 2 and Class 3 Systems Only]
For each encrypted communication link identified in Section 2.2.1 Communications Links, describe the key management system including key and re-key schemes and the protection of stored keys.

4.5 Preventative Measures and Immediate Actions

4.5.1 Preventative Security Measures [Class 2 and Class 3 Systems Only]
Describe the actions and procedures which the license will take to evaluate the security systems detailed within the DPP. Potential actions include network penetration testing, third party evaluation, IT security programs, employee training and software programs. Identify the proactive methods in which testing of preventative security measures will be performed to validate security, as well as the frequency with which the tests are to be performed.

4.5.2 Immediate Actions
Describe in detail planned immediate actions which the licensee will execute in response to a breach of security measures outlined within the DPP. In addition, detail the timeline and process through which the licensee will notify the licensing authority.

5. RESTRICTED OPERATIONS

5.0.1 Geographic Exclusion Areas [Class 2 and Class 3 Systems Only]
If this capability has been requested and NOAA approved provide a description of the process for restricting collection and dissemination of remote sensing data of geographic exclusion areas (GEA) as required within the remote sensing license.

5.0.2 Night Time Imaging [Class 2 and Class 3 Systems Only]
If this capability has been requested and NOAA approved provide a description of the process for restricting collection and dissemination of remote sensing data, categorized as night time imaging (NTI), as required within the remote sensing license.

5.0.3 Non-Earth Imaging [Class 2 and Class 3 Systems Only]
If this capability has been requested and NOAA approved provide a description of the process for restricting collection and dissemination of remote sensing data, categorized as non-Earth imaging (NEI), as required within the remote sensing license.
5.0.4 State of Israel [Class 2 and Class 3 Systems Only]

Provide a description of the process for restricting dissemination of remote sensing data, of the State of Israel (SOI) or its occupied territories, as required within the remote sensing license.
Appendix

A. DATA PROTECTION PLAN CLASSES

The data protection classes are a tool to assist NOAA in allocating the appropriate level of scrutiny for evaluation of an applicant’s Data Protection Plan. Systems which are classified as Class 2 or Class 3 warrant an increased level of scrutiny due to their potential to impact national security and require additional information from the licensee.

A.1 Class 1

Space systems subjected to Class 1 scrutiny are those for which the following assertions are true:

1) Sensors produce data which is not sensitive and which may be freely distributed to customers without restriction or post-processing.
   a) There is no expectation that systems will be subject to restrictions regarding the time and place from which data is collected.
2) Loss of space vehicle control to an unauthorized and malicious actor would not pose any reasonable hazard to the peaceful use of space.

A.2 Class 2

Space systems subjected to Class 2 scrutiny are those for which the following assertions are true and for which the government has clearly and reasonably articulated its rationale:

1) Sensors produce sensitive data which is equal or superior to the best examples of non-US or non-regulated sources but which, in general, may be freely distributed to all customers without restriction or post-processing to degrade quality.
   a) The time and place from which data is collected may be subject to restrictions where necessary to protect national security.
   b) Sensitive data does not include data that is freely or readily available from alternative sources such as aerial photography, cell phones, publicly available datasets or non-US commercial remote sensing systems.

A.3 Class 3

Space systems subjected to Class 3 scrutiny are those for which the following assertions are true and for which the government has clearly and reasonably articulated its rationale:

1) Sensors produce very sensitive data for which unauthorized dissemination would pose a clear and significant threat to national security. Licensing restrictions may require post-processing prior to distribution to some customers or restrict distribution to authorized customers.
   a) The time and place from which data is collected may be subject to restrictions where necessary to protect national security.
   b) Sensitive data does not include data that is freely or readily available from alternative sources such as aerial photography, cell phones, publicly available datasets or non-US commercial remote sensing systems.

2) Loss of space vehicle control to an unauthorized and malicious actor would pose a credible and significant hazard to the peaceful use of space.
B. DPP REQUIREMENTS TRACEABILITY

B.1 Requirement for a Data Protection Plan
Derived requirement per 15 CFR, Section 960.11(b)(13).

B.2 Requirement for Space Segment Data

B.2.1 Orbital Information
Derived requirement per 15 CFR, Section 960.11(b)(1).

B.2.2 On-Board Propulsion
Derived requirement per 15 CFR, Section 960.11(b)(1).

B.2.3 Sensor
Derived requirement per 15 CFR, Section 960.11(b)(1).

B.2.4 Communications Links
Derived requirement per 15 CFR, Section 960.11(b)(1), Section 960.11(b)(2), and Section 960.11(b)(13)(ii).

B.2.5 Link Characteristics
Derived requirement per 15 CFR, Section 960.11(b)(1), Section 960.11(b)(2), and Section 960.11(b)(13)(ii).

B.3 Requirement for Ground Segment Data

B.3.1 Ground Segment Locations
Derived requirement per Section 960.11(b)(2) and Section 960.11(b)(13)(ii).

B.4 Requirement for Security Plan

B.4.1 General Security Measures
Derived requirement per 15 CFR, Section 960.11(b)(2).

B.4.2 Cryptographic Hardware
Derived requirement per 15 CFR, Section 960.11(b)(2).

B.4.3 Remote Sensing Data
Derived requirement per 15 CFR, Section 960.11(b)(13).

B.4.4 Personnel
Derived requirement per 15 CFR, Section 960.11(b)(2).

B.4.5 Command and Control
Derived requirement per 15 CFR, Section 960.11(b)(2).

B.4.6 Storage
Derived requirement per 15 CFR, Section 960.11(b)(13).

B.4.7 Encryption
Derived requirement per 15 CFR, Section 960.11(b)(2).
B.4.8 Key Management
Derived requirement per 15 CFR, Section 960.11(b)(2) and Section 960.11(b)(13).

B.4.9 Preventative Security Measures
Derived requirement per 15 CFR, Section 960.11(b)(2).

B.4.10 Immediate Actions to Breach of Security
Derived requirement per 15 CFR, Section 960.11(b)(11) and Section 960.11(b)(13)(iv).

B.5 Restricted Operations

B.5.1 Geographic Exclusion Areas
Derived requirement per 15 CFR, Section 960.11(b)(1).

B.5.2 Night Time Imaging
Derived requirement per 15 CFR, Section 960.11(b)(1).

B.5.3 Non-Earth Imaging
Derived requirement per 15 CFR, Section 960.11(b)(1).

B.5.4 State of Israel
Derived requirement per 15 CFR, Section 960.11(b)(1) and Public Law 104-201, Section 1064.

C. ACRONYMS AND ABBREVIATIONS

DPP Data Protection Plan
CFR Code of Federal Regulations
GEA Geographic Exclusion Areas
IT Information Technology
NOAA National Oceanic and Atmospheric Administration
NEI Non-Earth Imaging
NTI Night Time Imaging
SOI State of Israel
ΔV Magnitude of the change to the space vehicle velocity vector produced by the propulsion system