

Introduction to Cybersecurity for Commercial Satellite Operations

Matthew Scholl
*Computer Security Division
Information Technology Laboratory*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8270-draft>

June 2021



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
*James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce
for Standards and Technology & Director, National Institute of Standards and Technology*

47 National Institute of Standards and Technology Interagency or Internal Report 8270
48 33 pages (June 2021)

49 This publication is available free of charge from:
50 <https://doi.org/10.6028/NIST.IR.8270-draft>

51 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
52 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
53 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best
54 available for the purpose.

55 There may be references in this publication to other publications currently under development by NIST in accordance
56 with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies,
57 may be used by federal agencies even before the completion of such companion publications. Thus, until each
58 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For
59 planning and transition purposes, federal agencies may wish to closely follow the development of these new
60 publications by NIST.

61 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to
62 NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at
63 <https://csrc.nist.gov/publications>.

64 **Public comment period: June 30, 2021 through ~~August 13~~ October 13, 2021**

65 National Institute of Standards and Technology
66 Attn: Computer Security Division, Information Technology Laboratory
67 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
68 Email: DraftIR8270Comments@nist.gov

69 All comments are subject to release under the Freedom of Information Act (FOIA).

70

71 **Reports on Computer Systems Technology**

72 The Information Technology Laboratory (ITL) at the National Institute of Standards and
73 Technology (NIST) promotes the U.S. economy and public welfare by providing technical
74 leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test
75 methods, reference data, proof of concept implementations, and technical analyses to advance
76 the development and productive use of information technology. ITL’s responsibilities include the
77 development of management, administrative, technical and physical standards, and guidelines for
78 the cost-effective security and privacy of other than national security-related information in
79 federal information systems.

80 **Abstract**

81 Space is an emerging commercial critical infrastructure sector that is no longer the domain of
82 only national government authorities. Space is an inherently risky environment in which to
83 operate, so cybersecurity risks involving commercial space – including those affecting
84 commercial satellite vehicles – need to be understood and managed alongside other types of risks
85 to ensure safe and successful operations. This report provides a general introduction to
86 cybersecurity risk management for the commercial satellite industry as they seek to start
87 managing cybersecurity risk in space. This document is by no means comprehensive in terms of
88 addressing all of the cybersecurity risks to commercial satellite infrastructure nor does it explore
89 risks to satellite vehicles, which may be introduced by implementing cybersecurity controls. The
90 intent is to introduce basic concepts, generate discussions, and provide sample references for
91 additional information on pertinent cybersecurity risk management concepts.

92 **Keywords**

93 commercial space satellite operations; cybersecurity; cybersecurity risk management; risk
94 management.

95 **Acknowledgments**

96 The authors wish to thank all contributors to this publication, especially Theresa Suloway,
97 Karen Scarfone and Greg Witte for their technical contributions, Scott Kordella for his tireless
98 assistance, and Isabel VanWyk for her outstanding technical editing.

99 **Audience**

100 The primary audience for this publication includes chief information officers (CIOs), chief
101 technology officers (CTOs), and risk officers of organizations who are using or plan to use
102 commercial satellite operations and are new to cybersecurity risk management for these
103 operations.

104 **Trademark Information**

105 All registered trademarks belong to their respective organizations.

106

107

Call for Patent Claims

108 This public review includes a call for information on essential patent claims (claims whose use
109 would be required for compliance with the guidance or requirements in this Information
110 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
111 directly stated in this ITL Publication or by reference to another publication. This call also
112 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications
113 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

114

115 ITL may require from the patent holder, or a party authorized to make assurances on its behalf,
116 in written or electronic form, either:

117

118 a) assurance in the form of a general disclaimer to the effect that such party does not hold
119 and does not currently intend holding any essential patent claim(s); or

120 b) assurance that a license to such essential patent claim(s) will be made available to
121 applicants desiring to utilize the license for the purpose of complying with the guidance
122 or requirements in this ITL draft publication either:

123 i. under reasonable terms and conditions that are demonstrably free of any unfair
124 discrimination; or

125 ii. without compensation and under reasonable terms and conditions that are
126 demonstrably free of any unfair discrimination.

127

128 Such assurance shall indicate that the patent holder (or third party authorized to make assurances
129 on its behalf) will include in any documents transferring ownership of patents subject to the
130 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
131 the transferee, and that the transferee will similarly include appropriate provisions in the event of
132 future transfers with the goal of binding each successor-in-interest.

133

134 The assurance shall also indicate that it is intended to be binding on successors-in-interest
135 regardless of whether such provisions are included in the relevant transfer documents.

136

137 Such statements should be addressed to: DraftIR8270Comments@nist.gov.

138

139 **Executive Summary**

140 As stated in the September 2018 United States National Cyber Strategy, the U.S. Government
141 considers unfettered access to and freedom to operate in space vital to advancing the security,
142 economic prosperity, and scientific knowledge of the Nation. However, cyber-related threats to
143 space assets (e.g., commercial satellites) and supporting infrastructure pose increasing risk to this
144 economic promise and commercial space emerging markets.

145 Commercial satellite operations occur in an inherently risky environment. Physical risks to these
146 operations are generally quantifiable and have the most likely potential to adversely impact the
147 businesses that operate commercial satellites, usually in low earth orbit. While this is the primary
148 risk consideration to satellite operations, continued growth in this new commercial infrastructure
149 allows for opportunities to address the cybersecurity risks along with the other risk elements.¹

150 Methods for the creation, maintenance, and implementation of a cybersecurity program for many
151 of the commercial and international markets include products in National and International
152 Standard-Setting Organizations (SSOs), as well as the use risk management guidance from the
153 National Institute of Standards and Technology (NIST). NIST risk management guidance
154 includes specific technical references, cybersecurity control catalogues, the IT Risk Management
155 Framework, and the Cybersecurity Framework (CSF).

156 The intent of this document is to introduce the CSF to commercial space businesses. This
157 includes describing a specific method for applying the CSF to a small portion of commercial
158 satellite operations (e.g., a small sensing satellite), creating an example CSF set of desired
159 security outcomes based on missions and anticipated threats, and describing an abstracted set of
160 cybersecurity outcomes, requirements, and suggested cybersecurity controls.

161 NIST asks the commercial satellite operations community to use this document as an informative
162 reference to assist in managing cybersecurity risks and to consider how cybersecurity
163 requirements might coexist within space vehicle system requirements. The example requirements
164 listed in this document could be used to create an initial baseline. However, NIST recommends
165 that organizations use this document in coordination with the set of NIST references and
166 applicable SSOs material to create cybersecurity outcomes, requirements, and controls
167 customized to support an organization's particular business needs and address its individual
168 threat models.

169 ***This report focuses on crewless commercial space vehicles that will not dock with human-***
170 ***occupied spacecraft.***

171

¹ These can include, but are not limited to, physical risks, EMI/EMC, financial risks, and supplier and customer risks.

172 **Table of Contents**

173 **Executive Summary iv**

174 **1 Introduction 1**

175 1.1 Purpose and Scope 1

176 1.2 Report Structure 1

177 **2 Conceptual High-Level Architecture of Satellite Operations 3**

178 **3 An introduction to the Cybersecurity Framework..... 7**

179 **4 Creating a Cybersecurity Program for Space Operations 10**

180 4.1 Using the Cybersecurity Framework 10

181 4.2 Case Study Example 11

182 4.3 Conclusion 20

183 **References 21**

184 **List of Appendices**

185

186 **Appendix A— Examples of Relevant Regulations 0**

187 **Appendix B— Acronyms 2**

188 **Appendix C— Glossary 0**

189 **List of Figures**

190

191 Figure 1. Major Parts of the Conceptual High-Level Architecture of Space Operations .. 4

192 Figure 2. Phases of Operations..... 6

193 Figure 3. The Cybersecurity Framework 7

194 Figure 4. Framework Core Structure 8

195 Figure 5. Example of the Identity Function showing the first category identity and access

196 management, along with the subcategories and informative references..... 9

197 **List of Tables**

198

199 Table 1: Control Table for Addressing Outcomes Countering Threat Models 15

200

201 **1 Introduction**

202 The concept of a commercial space sector has been evolving for some time. In 2007, the U.S.
203 Leadership in Space Commerce Strategic Plan stated,

204 From television and data communications, to personal navigation, to internet-based
205 satellite imagery, space commerce has enabled countless new economic benefits for our
206 nation. In addition, the expansion of the global market for commercial space capabilities
207 has generated robust worldwide competition. [3]

208 The White House National Space Policy stated this in 2010:

209 The term ‘commercial,’ for the purposes of this policy, refers to space goods, services, or
210 activities provided by private sector enterprises that bear a reasonable portion of the
211 investment risk and responsibility for the activity, operate in accordance with typical
212 market-based incentives for controlling cost and optimizing return on investment, and
213 have the legal capacity to offer these goods or services to existing or potential
214 nongovernmental customers. [4]

215 Today, space continues to be an emerging commercial sector that is no longer the domain of only
216 national government authorities. The commercial uses of space for research and development,
217 material sciences, communication, and sensing are growing in size, scale, and importance for the
218 future of the U.S. economy. Space is an inherently risky environment in which to operate, so
219 cybersecurity risks involving commercial space need to be understood and managed alongside
220 other types of risks to ensure safe and successful operations.

221 **1.1 Purpose and Scope**

222 This report provides a general introduction to cybersecurity risk management to the commercial
223 space commerce industry. This document is by no means comprehensive in terms of addressing
224 all cybersecurity risks to commercial space infrastructure, nor does it explore how cybersecurity
225 solutions might introduce risk to a space vehicle. The intent is to introduce basic concepts,
226 generate discussions, clear confusion, and provide references for additional information on
227 pertinent cybersecurity risk management concepts. *This report focuses on crewless commercial*
228 *space vehicles that will not dock with human-occupied spacecraft.*

229 **1.2 Report Structure**

230 The rest of this report is organized into the following sections and appendices:

- 231 • Section 2 provides a notional, conceptual, high-level architectural view of commercial
232 satellite operations.
- 233 • Section 3 describes the steps of the Cybersecurity Framework and provides a notional
234 example of how a satellite organization might apply those steps.

235

236 • Appendix A provides examples of regulations that may be relevant for commercial
237 satellite operations.

238 • Appendix B lists the acronyms used in the report.

2 Conceptual High-Level Architecture of Satellite Operations

240 This section provides a notional, conceptual, high-level architectural view of commercial,
241 crewless space operations. This view can be helpful in understanding, assigning, and managing
242 cybersecurity requirements and risks associated with different owners and operators of different
243 parts of the architectures. This architecture can be under the sole control of one system owner or
244 shared among numerous owners, including public, commercial, and private.

245 Once in operation, space vehicles share an ecosystem that has no national and few natural
246 boundaries and where safety is a communal concern. For the purposes of this paper and to
247 facilitate subsequent discussions in setting, expressing, or meeting cybersecurity requirements,
248 NIST notionally defines the scope of a commercial space operations architecture to include the
249 following:

250 Space Architecture Segments

251 **Ground Segment:** *Ground operations* are terrestrial-based activities that can be
252 automated or conducted by human operators. They often include some or all of the space
253 operations (i.e., station keeping and payload commanding) and can be co-located with
254 launch facilities or at a separate set of facilities. Ground operations can be outsourced in
255 whole or in part. Even at launch, the payload operator may not be collocated with the
256 launch facility.

257 **Link Segment:** *Command and control* are the signaling operations sent to the satellite to
258 conduct a mission function, perform diagnostics, reset the state of the equipment, and/or
259 activate the propulsion systems of the vehicle. Command and control operations are
260 generated on the ground and can be transmitted to the vehicle in several ways. The
261 commands may be sent via a fiber link to a remote ground station, which then transmits
262 the commands via a direct RF or optical link to the satellite from the ground. The second
263 method uses a set of space relays, where the original commands are sent from the ground
264 via RF or optical to a relay satellite and then transmitted via RF or optical to the target
265 satellite. Finally, mobile devices and technologies not associated with a specific ground
266 operations location, such as intra-vehicle communications, can be used to deliver
267 commands to a satellite or its payload.

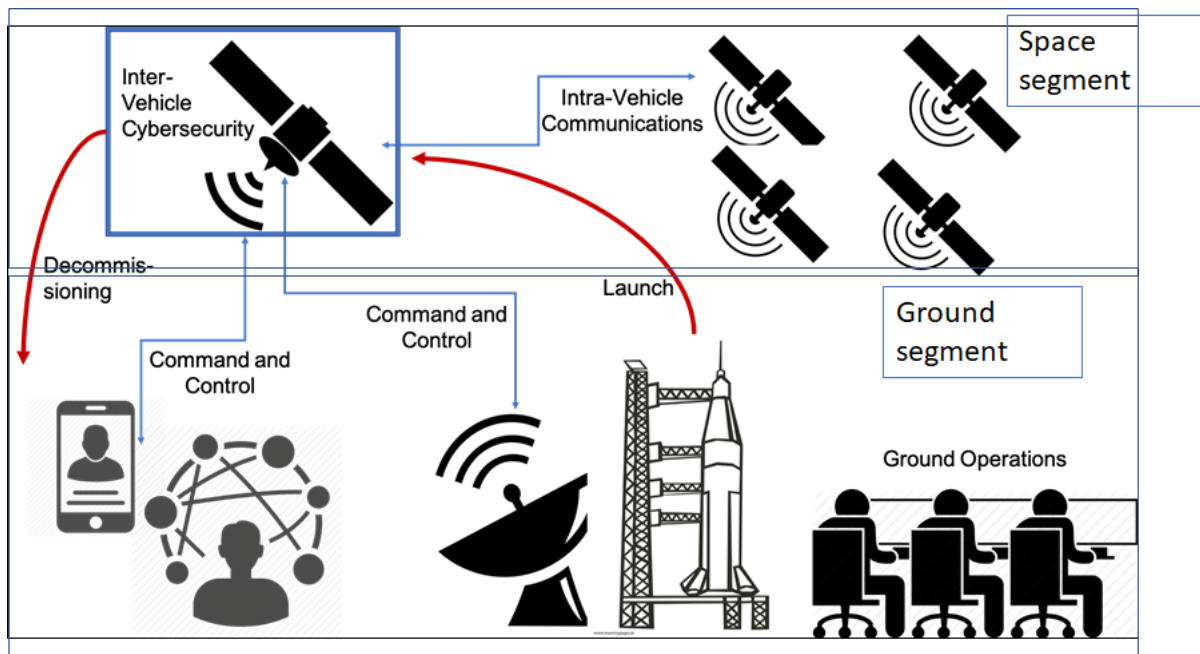
268 **User Segment:** These are consumers, such as GPS receivers, satellite phone users, or
269 satellite TV receivers.

270 **Space Segment:** *The space vehicle consists of the satellite (BUS) and one or more*
271 *payloads. The BUS consists of the components of the vehicle associated with the “flying*
272 *of the satellite,” such as power, structure, attitude control system, processing and*
273 *command control, and telemetry. The spacecraft can carry many specialized payloads to*
274 *conduct missions, including remote sensing and communications. The BUS and the*
275 *payload generally combine to form the satellite.*

276 **Inter-Vehicle Cybersecurity:** *Inter-vehicle cybersecurity* refers to the cybersecurity
 277 capabilities of the satellite vehicle itself, including its ability to protect itself against
 278 cybersecurity threats, detect threat actions, respond to cybersecurity attacks, and recover
 279 when necessary. These capabilities should be designed as part of security development
 280 and integrated early in the system life cycle. Often, inter-vehicle cybersecurity is the
 281 primary responsibility of small commercial satellite owners and operators, and much of
 282 the rest of the architecture is outsourced to external suppliers and providers.

283 **Intra-Vehicle Communications:** Communications between operational satellites for
 284 mission functions – such as command and control, networking of compute capabilities,
 285 redundancy of operations and mission functions, tracking, and communications – are
 286 known as *intra-vehicle communications*. Therefore, the integrity and authenticity of these
 287 communications is critical.

288



289

290 **Figure 1. Major Parts of the Conceptual High-Level Architecture of Space Operations**

291 Figure 1 reflects major parts of the conceptual, high-level architecture of satellite operations.
 292 This architecture is for crewless spacecraft and does not include cybersecurity requirements for
 293 human space systems, spacecraft, or systems that will dock with human systems and/or lunar
 294 landers.

295 **Spacecraft Vehicle Life Cycle Phases**

296 The space vehicle will experience different phases of operations, each of which may have unique
297 risks that need to be addressed.

298 **Assembly:** Spacecraft components are procured from across the world and brought
299 together to allow the spacecraft to perform various missions. Hardware and software
300 supply chain is, therefore, a critical component of cybersecurity. Once vehicles are
301 launched, the ability to modify hardware is limited, if not impossible. Hardware implants
302 or vulnerabilities are difficult to mitigate and can have a foundational impact on
303 cybersecurity. However, software on a space vehicle can often be patched or modified
304 from the ground.

305 **Prelaunch:** This is a critical time for the vehicle, when operators will be testing RF links
306 as well as the utilization of an umbilical cord to the launch vehicle for diagnostics and
307 telemetry. It is important for operators to understand the connectivity and access that the
308 various satellite health monitoring systems have during prelaunch.

309 **Launch:** *Launch* is the phase of space commerce that entails moving the space system to
310 its operational environment – generally in low Earth orbit (LEO) – from a pad, rack,
311 ramp, or other device or installation. Launch can include launch devices and installations,
312 fuel operations and storage, and launch safety and destruct systems. Launch can have
313 significant overlap with ground operations, and the two are often combined. However,
314 due to the current cost, complexity, and safety concerns associated with launch, it is often
315 outsourced to small commercial satellites.

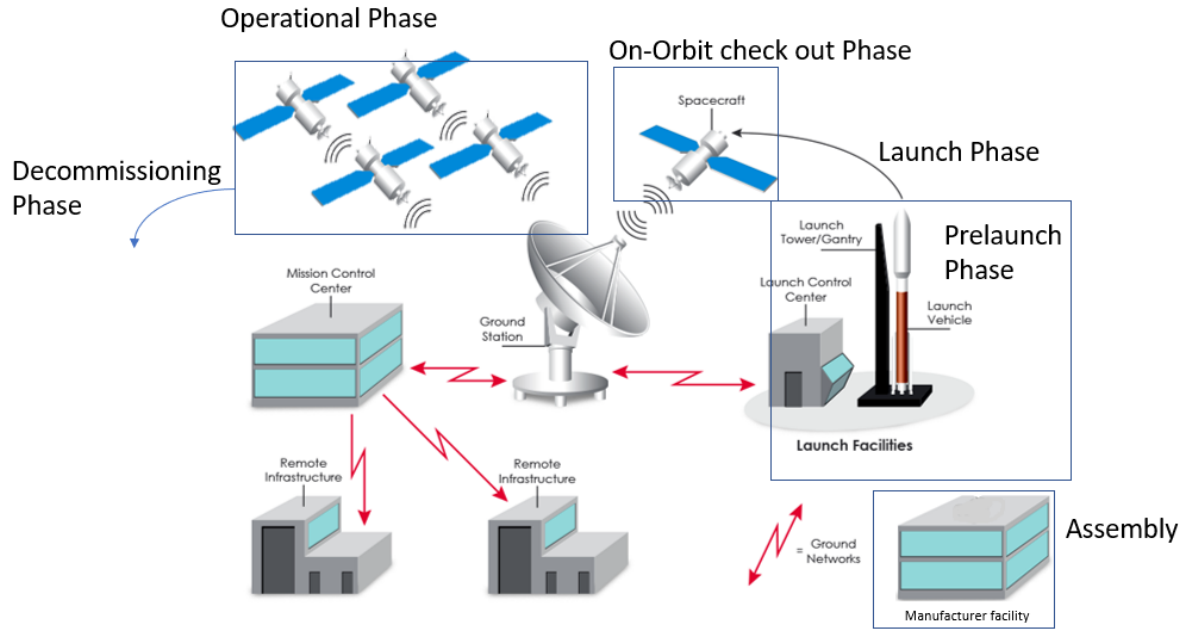
316 **On-orbit check out:** Once the satellite is placed into orbit, the satellite must beacon and
317 establish a link to the ground command and control system. The satellite typically
318 undergoes several checks to make sure that the system has survived launch and that all
319 systems are operational. Once this has occurred, the satellite will enter operational status.

320 **Operations – Sensing, Information Processing, Data Acquisition, and**
321 **Communication:** The satellite conducts a mission operation that involves some function
322 or combination of functions for sensing, information processing, data acquisition, and
323 communication. These are functional requirements directly related to the business
324 mission of the satellite and are conducted by the satellite and/or its payloads.

325 **Decommissioning:** Decommissioning of a commercial satellite is a high-risk endeavor
326 with requirements for the post-mission disposition of satellites. General good practices
327 include maintaining control of orbital debris released during normal operations,
328 minimizing debris generated by accidental explosions, and ensuring the post-mission
329 disposal of space structures. Decommissioning other areas of the space operations
330 architecture can include the need to handle and dispose of sensitive materials, intellectual
331 property, and hazardous materials. The cybersecurity risks of decommissioning should

332 consider appropriate confidentiality, integrity, and availability considerations as well as
333 related physical threats to commercial satellite systems once decommissioned.

334



335

336

Figure 2. Phases of Operations

337

338

339

3 An introduction to the Cybersecurity Framework

341 The Cybersecurity Framework was developed in response to Executive Order 13636, *Improving*
342 *Critical Infrastructure Cybersecurity*. The framework is based on a risk management approach to
343 cybersecurity that can be tailored to various industries. It provides common terminology and a
344 methodology that can be implemented by organizations based on their resources and business
345 needs. The Cybersecurity Framework consists of five functions: identify, protect, detect, respond,
346 and recover. The functions are shown in a circular format to communicate to the user that
347 cybersecurity is a continuous process that enables an organization to navigate the changing
348 landscape of cybersecurity risks.



349

350

Figure 3. The Cybersecurity Framework

351 In addition to the five primary functions of the Cybersecurity Framework, there are categories
352 and subcategories that express cybersecurity outcomes and informative references to assist in the
353 implementation of controls that can achieve those outcomes. A breakdown of the CSF can be
354 visualized in Figure 4.

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

355

356

Figure 4. Framework Core Structure

357 To help explain the context of the categories, subcategories, and informative references, an
 358 example of the first row of *identify* with the category of identity and access management is
 359 provided in Figure 5. Each category has associated subcategories, which provide specific
 360 outcomes. The last column of information references provides references for that particular
 361 outcome that cite applicable NIST and SSO references.

362

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	<ul style="list-style-type: none"> - CCS CSC 1 - COBIT 5 BAI09.01, BAI09.02 - ISA 62443-2-1:2009 4.2.3.4 - ISA 62443-3-3:2013 SR 7.8 - ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 - NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	<ul style="list-style-type: none"> - CCS CSC 2 - COBIT 5 BAI09.01, BAI09.02, BAI09.05 - ISA 62443-2-1:2009 4.2.3.4 - ISA 62443-3-3:2013 SR 7.8 - ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 - NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	<ul style="list-style-type: none"> - CCS CSC 1 - COBIT 5 DSS05.02 - ISA 62443-2-1:2009 4.2.3.4 - ISO/IEC 27001:2013 A.13.2.1 - NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	<ul style="list-style-type: none"> - COBIT 5 APO02.02 - ISO/IEC 27001:2013 A.11.2.6 - NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	<ul style="list-style-type: none"> - COBIT 5 APO03.03, APO03.04, BAI09.02 - ISA 62443-2-1:2009 4.2.3.6 - ISO/IEC 27001:2013 A.8.2.1 - NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<ul style="list-style-type: none"> - COBIT 5 APO01.02, DSS06.03 - ISA 62443-2-1:2009 4.3.2.3.3 - ISO/IEC 27001:2013 A.6.1.1 - NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

363

364
365

Figure 5. Example of the Identity Function showing the first category identity and access management, along with the subcategories and informative references

366

4 Creating a Cybersecurity Program for Space Operations

The application of high-level processes from the Cybersecurity Framework may help satellite operators with the creation and maintenance of a cybersecurity program. While the overall process is applicable to all parts of commercial space architectures and phases of operations, this document also provides a notional example of applying the CSF to generating cybersecurity requirements for the satellite during sensing, information processing, data acquisition, and communication to illustrate how these steps are used and to derive example cybersecurity outcomes, requirements, and controls for this specific use.

4.1 Using the Cybersecurity Framework

While only a few organizations will own or control all aspects of space operations, the Cybersecurity Framework helps with organizing and communicating about cybersecurity risks and activities. The Framework can be used to communicate cybersecurity requirements to suppliers and to manage how risk is mitigated, managed, transferred, or accepted when outsourcing one or more parts of space operations.

Commercial space operations can be hybrid modes with few organizations owning or controlling all parts of space operations. Therefore, communicating clear expectations, capabilities, and requirements across the different owners of the space operations scope is important for understanding and managing cybersecurity risks.

Step 1: Establish Scope and Priorities. It is most effective to address cybersecurity in the earliest stages of building the components of the space architecture and embedding risk-reducing measures that meet organizational mission and business objectives into the design and supply chain. However, many commercial satellite operators have already deployed several generations of their vehicles, and many parts of an architecture are in use.

For companies that have already begun deployment, a current cybersecurity profile should be created to describe what cybersecurity outcomes are being achieved. A target profile can be created to describe the outcomes needed to meet the cybersecurity risk management goals of the organization. A gap analysis of the differences between the current profile versus the target profile provides information that the organization can use to make decisions regarding cybersecurity.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for mission and business needs, the organization identifies related systems, assets, regulatory requirements,² and its overall risk approach. The organization then works to identify threats and vulnerabilities applicable to those systems and assets.

² Some examples of regulatory requirements can be found in Appendix A.

400 **Step 3: Create a Current Profile.** This step allows the organization to understand their current
401 cybersecurity posture. An organization can assess how it is currently implementing the CSF
402 functions by creating a Current Profile: a list of subcategory activities that are currently being
403 implemented within the organization.

404 **Step 4: Conduct a Risk Assessment.** This assessment could be guided by the organization's
405 overall risk management process or previous risk assessment activities. The organization
406 analyzes the operational environment, identifies emerging risks, and uses cyber threat
407 information from internal and external sources to discern the likelihood of a cybersecurity event
408 and the impact that the event could have on the organization.

409 **Step 5: Create a Target Profile.** The organization creates a Target Profile by selecting the
410 subcategories that support the organization's desired cybersecurity outcomes. Each organization
411 will have a unique risk posture, which will result in a unique set of subcategories.

412 **Step 6: Determine, Analyze, and Prioritize Gaps.** The organization compares the Current
413 Profile and the Target Profile to identify potential gaps. It then creates a prioritized action plan to
414 address those gaps.

415 **Step 7: Implement Action Plan.** The organization determines which actions to take to address
416 the gaps.

417 **4.2 Case Study Example**

418 This section provides a short example walk-through using the Cybersecurity Framework steps
419 for a notional low Earth orbit (LEO) "small satellite vehicle," which represents only one portion
420 of larger space operations. The same process³ can be applied to the other areas of space
421 operations, if needed. In this notional example, a Framework Profile is created to address the
422 core cybersecurity areas below:

- 423 • **Identify** assets, threat models, and regulatory requirements.
- 424 • **Protect** assets using outcomes that are then traced to controls and standards.
- 425 • **Detect** cybersecurity issues and threats as they materialize.
- 426 • **Respond** to those threats.
- 427 • **Recover** from incidents.

428 *For Step 1* – The notional use case is scoped to just the following aspects of Figure 1: the
429 satellite vehicle itself, Inter-Vehicle Cybersecurity, Command and Control, and Sensing,
430 Information Processing, and Data Acquisition. The notional company only owns and controls the
431 satellite vehicle part of the operations. They will use its generated target profile to express

³ It is important to note that the CSF is not prescriptive about how the steps should be applied, and this use case is intended for use as one of many possible methods.

432 cybersecurity requirements for their vehicle and to compare products and services offered for
433 other areas of space operations that are hybrid and/or outsourced.

434 *For Step 2* – The organization’s business leaders identify relevant regulatory requirements and
435 critical systems, and they model potential high-level threats (and their potential impacts). The
436 organization defines its critical systems as those with a direct impact on the satellite itself, as
437 well as their business model, which acquires “data over a geographic area.” Organizational
438 leadership determines that the business and mission-critical systems are:

- 439 • Communications technologies
- 440 • Guidance control
- 441 • Sensor systems

442 The organization then generates a high-level cybersecurity risk model that can be help identify
443 its most severe cybersecurity vulnerabilities, the threat events that are most likely occur, and
444 events that could have the highest negative impact on the business. This analysis is less rigid
445 than the detailed risk evaluation that occurs in Step 4 and is intended to spur discussion regarding
446 the types of risk events that might have some impact on the organization. The resulting risk
447 understanding helps in shaping the Current State Profile described in Step 3.

448 A list of the events and the business impacts is then generated:

<i>Cybersecurity Events</i>	<i>Business Impacts</i>
Intentional jamming and spoofing of sensor data	loss of data assets for customers
Interception and theft of sensor data	loss of markets and customers
Intentional corruption of sensor systems	loss of satellite vehicle
Jamming of guidance control	loss of satellite vehicle
Hijacking and unauthorized commands to guidance control	loss of satellite vehicle
Malicious code injection	loss of satellite vehicle, data corruption, and data loss
Denial-of-service attack	loss of data and/or loss of guidance

449
450 To mitigate these high-impact, high-probability events, a set of needed cybersecurity outcomes is
451 generated. These are, in effect, the inverse of the threat models to the critical systems and are
452 placed in the terms used in the core of the CSF where they are most appropriate for the
453 outcomes. An example is below:

- 454 • *Protect/Detect/Respond/Recover* from jamming, spoofing, and data interception of
455 communication technologies;
- 456 • *Protect/Detect/Respond/Recover Guidance Control* from unauthorized access,
457 unauthorized commands, and unauthorized jamming;
- 458 • *Protect/Detect/Respond/Recover* from spoofing, interception, and the corruption of
459 sensor data;
- 460 • *Protect/Detect/Respond/Recover Satellite Operations* from malicious code attacks; and,
461 • *Protect/Detect/Respond/Recover* communication technologies, sensors, and guidance
462 controls from denial-of-service attacks.

463 Regulations and other requirements for each component of operations, specifically for the
464 sensing satellite vehicle, are identified and used to generate outcomes that are added to the above
465 list when needed. These are then tagged to identify their sources as regulatory and to ensure that
466 any needed records are generated and maintained on the implementation of these requirements.

467 Currently, many federal agencies hold oversight over and requirements in different elements of
468 space operations. These are the primary inputs for identifying initial cybersecurity requirements
469 for space commerce systems. Some examples of relevant regulations are described in Appendix
470 A.

471 *For Step 3* – Assume that the only current cybersecurity implementation is that driven by
472 regulatory requirements. In the example use case, these are the NOAA requirements for the
473 licensing of Private Remote Sensing Space Systems. The organization will need to assure and
474 state that:

475 The methods applicant will use to ensure the integrity of its operations, including plans
476 for: Positive control of the remote sensing space system and relevant operations centers
477 and stations; denial of unauthorized access to data transmissions to or from the remote
478 sensing space system; and restriction of collection and/or distribution of unenhanced data
479 from specific areas at the request of the U.S. Government.⁴

480 The organization documents the policies, processes, and technology that are in place, especially
481 those related to the high-level cybersecurity risk issues described in Step 2. The organization
482 should walk through all of the subcategories outlined in the Cybersecurity Framework and select
483 those that are currently in practice. The list of subcategories being addressed forms the “Current
484 Profile.” For the purposes of this example, the company has found that they are currently
485 implementing the following, which will serve as their “Current Profile”:

- 486 • PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited
487 for authorized devices, users, and processes.

⁴ <https://www.nesdis.noaa.gov/CRSRA/licenseHome.html>

- 488 • PR.AC-4: Access permissions and authorizations are managed, incorporating the
489 principles of least privilege and separation of duties.
- 490 • PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-
491 factor) commensurate with the risk of the transaction (e.g., individuals' security and
492 privacy risks and other organizational risks).
- 493 • PR.DS-1: Data at rest is protected.
- 494 • PR.DS-2: Data in transit is protected.
- 495 • PR.DS-4: Adequate capacity to ensure availability is maintained.
- 496 • PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and
497 information integrity.
- 498 • PR.IP-12: A vulnerability management plan is developed and implemented.
- 499 • PR.PT-5: Mechanisms (e.g., fail-safe, load balancing, hot swap) are implemented to
500 achieve resilience requirements in normal and adverse situations.
- 501 • DE.AE-3: Event data is collected and correlated from multiple sources and sensors.
- 502 • DE.CM-1: The network is monitored to detect potential cybersecurity events.
- 503 • DE.CM-4: Malicious code is detected.
- 504 • DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is
505 performed.

506 *For Step 4* – The organization prioritizes and validates the needed cybersecurity outcomes from
507 Step 3 and uses them to inform the specific technical cybersecurity controls to be selected to
508 meet those outcomes.

509 The organization considers the costs of cybersecurity mitigation and the potential risks addressed
510 in light of each subcategory recorded in the Current State Profile. The team consults various
511 authorities at the Department of Homeland Security and Department of Defense to better
512 understand potential threats to space-based network operations. The organization joins a local
513 Information Sharing and Analysis Center (ISAC) so that company representatives will have a
514 venue for sharing and receiving prioritized information regarding known risks as the threat and
515 technology landscapes evolve.

516 The organization applies the principles described in NIST SP 800-30, *Guide for Conducting Risk*
517 *Assessments*, to set a scale for likelihood and impact and to prioritize outcomes and controls that
518 can manage the risks with the most negative impacts and/or that are most cost-effective for their
519 risk management results. Supported by this information, the organization is then prepared to
520 determine the outcomes that will achieve the desired risk posture in a cost-effective way.

521 *For Step 5* – The organization creates the following Target Profile to express its satellite vehicle
522 Cybersecurity Requirements. Table 1 maps outcomes that address threats and associated
523 technical controls. An ordinal count is made for the amount of individual outcome and threat-
524 pairing that a control might address. This will further assist in establishing priorities and helping
525 with investment decisions. For example, one cybersecurity control might be effective in
526 achieving many of the outcomes sought. This information can assist in understanding priorities
527 as well as mitigations that might need stronger monitoring, detection, and recovery capabilities.

528 The creation of these outcome/threat-pairings with mitigation techniques also builds a list of
 529 references that can be used to express the specific technical requirements of the control. These
 530 include NIST references and those from other sources, such as Standard Development
 531 Organizations (SDOs), the Committee on National Security Systems Instructions (CNSSI) 1200,
 532 and others that are relevant to the organization.

533 **Table 1: Control Table for Addressing Outcomes Countering Threat Models**

Outcome	Threat	Mitigation Technique	CSF Subcategory	Potential 800-53r4 Control Reference	Potential 800-53r5 Control Reference
Protect communication technologies	Denial of service (DOS)	Authenticated communications	PR.AC-7 PR.DS-4	IA-1, 2,3,5,8 SC-5, AU-4	IA-1, 2,3,5,8 SC-5, AU-4
		Allow listing	PR.IP-1	PS 2,3,4,5,6 CM-7	CM-7
		System resilience	PR.PT-5	CP-2,7 SA-14	CP-7
	Spoofing	Authenticated communications	PR.AC-7 PR.DS-4	IA-1, 2,3,5,8	IA-1, 2,3,5,8
		Allow listing	PR.IP-1	PS 2,3,4,5,6 CM-7	CM-7
		Access control	PR.AC-1 PR.AC-3 PR.PT-3 PR.AC-6 PR.AC-7	AC-3, 8, 9,19	AC-3
		Encryption of data in transit	PR.DS-2	SC-8/SC-17	SC-8
	Data interception	Encryption of data in transit	PR.DS-2 PR.DS-4	SC-5, SC-8	SC-5,8
Detect threats to communication technologies	DOS		DE.CM-1	SC-5	SC-5
	Spoofing	Audit logs of communication activity	ID.SC-4 DE.DP-4	AU-2	
	Data interception	Encryption of data in transit	PR.DS-2 PR.DS-4	SC-5, SC-8	SC-5,8
Respond to threats to communication technologies	DOS	Use of secondary/alternate channels; log, report, share	RS.MI-1 PR.DS-4 PR.PT-1	IR-4	IR-4
	Spoofing	Log, report, share	PR.PT-1	AU Family	AU-1,2,3,6,7,12,13,14,16
	Data interception	Encryption of data in transit	PR.DS-2 PR.DS-4	SC-8, SC-11	SC-8,11

Outcome	Threat	Mitigation Technique	CSF Subcategory	Potential 800-53r4 Control Reference	Potential 800-53r5 Control Reference
Recover from Threats to Communications Technologies	DOS	Audit, Self/Health Testing	RC.IP-1	CP-10, IR-4, IR-8	CP-10, IR-4, IR-8
	Spoofing	Audit, Self/Health Testing	RC.IP-1	AU-2	
	Data Interception	Encryption of Data in Transit	RC.IP-1	SC-5, SC-8	SC-5, SC-8
Protect guidance control	Unauthorized access	Access control	PR.AC-4 PR.DS-1		
	Unauthorized commands	Authenticated communication	PR.AC-6 PR.AC-7	SC-8	SC-8
		Encryption of data in transit	PR.DS-2 PR.DS-4	SC-8	SC-8
	DOS	Authenticated communications	PR.AC-6 PR.AC-7	SC-8	SC-8
		Command signal allow listings	PR.IP-1	CM-7	CM-7
		System resilience/fail-safe	PR.PT-5		
	Detect threat to guidance control	Unauthorized access	Access logging and audit	DE.CM-4 PR.PT-1 PR.AC-7	AU-2/AC-7
	Unauthorized commands	Command logging and audit	DE.CM-4 DE.CM-7 PR.PT-4 PR.AC-7 PR.PT-1	AU-2/AC-7, SC-24	AU-2
	DOS	Drop unauthorized communications/fail-safe	PR.PT-5	AC-3, 8,9,19	AC-3
Respond to threats to guidance control	Unauthorized access	Forensic review of data and access areas; system lockout	RS.AN-3 RS.MI-1 PR.AC-7	AC-7	AC-7
	Unauthorized commands	Forensic review of command logs; system lockout	RS.AN-3 RS.MI-1 PR.AC-7 PR.PT-4	SC-24	
	DOS	Drop unauthorized communications/fail-safe	PR.AC-3, PR.AC-4 PR.PT-5	AC-3, 8,9,19	AC-3
Recover to threats to guidance control	Unauthorized access	Access credential rotation and refresh	PR.AC-1, PR.AC-6, PR.AC-7	AC-3, 8,9,19	AC-3

Outcome	Threat	Mitigation Technique	CSF Subcategory	Potential 800-53r4 Control Reference	Potential 800-53r5 Control Reference
	Unauthorized commands	Access credential rotation and refresh	PR.AC-1, PR.AC-6, PR.AC-7	AC-3, 8,9,19	AC-3
	DOS		PR.PT-4, PR.PT-5		
Protect sensor data	Spoofing	Encryption of data in transit	PR.DS-2	SC-8	SC-8
	Corruption	Message authentication	PR.AC-7	SC-8	SC-8
		Digital signature	PR.AC-6	SC-8	SC-8
	Interception	Encryption of data in transit	PR.DS-2	SC-8	SC-8
	DOS	Fail-safe/store and send	PR.PT-5 PR.DS-1 PR.DS-6	SI-7	SI-7
Detect threats to sensor data	Spoofing	Detect unauthorized access to data; encryption	DE.CM-1 DE.AE-3 DE.CM-7	SC-5	SC-5, CM-3, 8
	Corruption	Data reference checks	DE.AE-3	SC-5	SC-5, CM-3, 8
	DOS	Data type allowlistings	DE.CM-7	CM-7	SC-5, CM-3, 8
Respond to threats to sensor data	Spoofing	Data quality checks	RS.AN-1 RS.AN-3	AC-7	
	Corruption	Data quality checks	RS.AN-1 RS.AN-3	AC-7	AU-7, IR-4
	Interception	Encryption	PR.DS-2	SC-8	SC-8
	DOS	ReXmit/Data ACK, HMACs/CRCs	PR.PT-4, PR.PT-5	AC-4, AC-17, SC-7	
Recover from threats to sensor data	Spoofing	Restore systems or assets	RC.IP-1	CP-10, IR-4, IR-8	CP-10, IR-4, IR-8
	Corruption	Restore systems or assets	RC.IP-1	CP-10, IR-4, IR-8	CP-10, IR-4, IR-8
	Interception	Restore systems or assets	RC.IP-1	CP-10, IR-4, IR-8	CP-10, IR-4, IR-8
	DOS	Restore systems or assets	RC.IP-1	CP-10, IR-4, IR-8	CP-10, IR-4, IR-8
Protect satellite operations	Malicious code	Secure engineering	PR.IP-1 PR.IP-3	CM-3, 4, 10	CM-3, 4, 10

Outcome	Threat	Mitigation Technique	CSF Subcategory	Potential 800-53r4 Control Reference	Potential 800-53r5 Control Reference
		Independent bus design	PR.PT-5	CP-7	
		Malware detection	PR.DS-6	SI-7	SI-7
		Input constraints/allow listings	PR.PT-3	AC- 3	AC-3 , 7
		BIOS security	PR.DS-6, PR.DS-8	SI-7	SI-7
		Secure update	PR.DS-6 PR.IP-12	SI-7	SI-7
Detect threats to satellite operations	Malicious code	AV/Health checks	DE.CM-4, DE.CM-7	AU-2, AC-7	
Respond to threats to satellite operations	Malicious code	Alternate safety check methods	RS.AN-1 RS.AN-3 RS.MI-1	AC-7	
Recover to threats to satellite operations	Malicious code	Secure update/reinstall; verify data sets; self-testing	RC.IP-1	CP-10, IR-4, IR-8	CP-10, IR-4, IR-8

534

535 *For Step 6* – The organization determines a new cybersecurity baseline, and each row in the
536 Target Profile will be part of the new action plan. In subsequent iterations, this step will identify
537 gaps between the current and target states and will provide an opportunity to add or update plans.

538 In light of the desired state, as described in the profile, the following action plans for protecting
539 the cybersecurity of the satellite vehicle service is created.

540 **To protect the satellite and its data from communications spoofing, interception,**
541 **corruption, tampering, and denial of service:**

- 542 1. Only allow authorized devices to communicate with the satellite, and employ the
543 following requirements:
- 544 a. Authenticate the claimed identity of any device attempting to communicate. CSF:
545 PR.AC-1, PR.AC-6, PR.AC-7
 - 546 b. Drop all communication attempts for which the access authorization of the other
547 device cannot be confirmed. CSF: PR.AC-3, PR.AC-4
 - 548 c. Check the integrity of communications and drop any communications where integrity
549 appears to have been violated. CSF: PR.DS-2
- 550 2. Only allow authorized devices to access sensitive data within the satellite’s
551 communications.

- 552 a. Use encryption to protect the contents of communications. CSF: PR.DS-2, PR.DS-4
553 b. Require that the recipient of encrypted communications be authenticated before they
554 can decrypt the communications and access their contents. (See 1a above.)
555 3. Make the satellite’s communications resilient to adverse conditions.
556 a. Use communication protocols that ensure delivery. CSF: PR.PT-5
557 b. Have a secondary or alternate communications channel available at all times, and
558 automatically fail over to it when the primary communications channel is not
559 functioning properly. CSF: PR.PT-5
560 c. When communications are unavailable, store any unsent sensor data and send it after
561 communications are restored. CSF: PR.PT-5
562 4. Build protections into the satellite to thwart DDoS-related connection attempts. CSF:
563 PR.PT-4, PR.PT-5

564 **To protect the satellite and its data from unauthorized access, use, corruption, tampering,**
565 **and denial of service:**

- 566 1. Use secure device design and development practices for the satellite hardware, firmware,
567 operating system, and applications.
568 a. Isolate executing processes from each other. See the SSDF publication.
569 b. Validate all input, including commands and data (e.g., allow listings, input
570 constraints). See the SSDF publication.
571 c. Satellites typically have multiple redundant paths to account for failures in orbit. For
572 example, the MIL-STD-1553 data bus has multiple redundant paths. The standard
573 also calls for an “A” side and a “B” side for space vehicles and associated redundant
574 hardware that will allow the satellite to operate if any component fails. The isolation
575 of the data bus is logical, not physical, and space operators should consider isolation
576 as part of their design, understanding the SWAP (i.e., size, weight, and power)
577 impacts that this may produce.
578 d. Build protections into the device for DoS attacks.
579 2. Prevent and deter attacks against the satellite.
580 a. Use a hardware root of trust to perform a secure boot, which will be the basis for
581 verifying BIOS security and conducting system integrity checks and other health
582 checks/self-tests. CSF: PR.DS-6, PR.DS-8
583 b. Provide update, upgrade, and uninstall capabilities for firmware and software. (Also
584 see items 1 and 2 above.) CSF: PR.IP-12
585 c. Configure the satellite to avoid known security weaknesses. CSF: PR.IP-1, PR.IP-3

- 586 d. Prevent unauthorized software from executing (e.g., anti-malware software,
587 application allow listings software, code signing). CSF: DE.CM-4, DE.CM-7, PR.PT-
588 3
- 589 3. Only allow authorized parties to access and alter sensor data stored on the satellite.
- 590 a. Enforce the principle of least privilege. CSF: PR.AC-4, PR.DS-1
- 591 b. Protect the integrity of all stored sensor data. CSF: PR.DS-1, PR.DS-6

592 **To detect, respond to, and recover from attacks and incidents involving the satellite, its**
593 **data, and its communications:**

- 594 1. Log security-related events, and continuously review the logs. CSF: PR.PT-1, DE.AE-3,
595 DE.CM-1
- 596 2. Investigate suspicious events. CSF: DE.DP-4, RS.AN-1, RS.AN-3
- 597 3. Prevent an incident from continuing or expanding (e.g., by failing safe). CSF: RS.MI-1
- 598 4. Recover from incidents by restoring data and software. RC.IP-1

599

600 *For Step 7* – Security leaders present the action plan to key company stakeholders for approval.
601 The business case and requests for appropriate resources are presented to the executives for
602 approval of the plan. Processes to monitor and review the plan’s implementation ensure that the
603 activities sufficiently address cybersecurity risks to satellite operations, allow for future updates
604 to the profiles, and maintain oversight over external service providers.

605

606 **4.3 Conclusion**

607 NIST has provided this example to show how an organization might apply the steps of the
608 Cybersecurity Framework to evaluate and address possible security risks. NIST recommends that
609 organizations apply the steps that best apply to their threat models, business cases, and risk
610 tolerance. As the industry expands, NIST will continue to support the community through
611 research products and risk management guidance.

References

- [1] National Institute of Standards and Technology (2001) Security requirements for cryptographic modules (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publications (FIPS PUBS) 140-2, Change Notice 2 December 03, 2002. <https://doi.org/10.6028/NIST.FIPS.140-2>
- [2] Joint Task Force Transformation Initiative Interagency Working Group (2013) Security and privacy controls for federal information systems and organizations (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. <https://doi.org/10.6028/NIST.SP.800-53r4>
- [3] National Oceanic and Atmospheric Administration (2007) U.S. Leadership in Space Commerce: Strategic Plan for the Office of Space Commercialization (OSC) (U.S. Department of Commerce). Available at <https://www.space.commerce.gov/wp-content/uploads/NOAA-2007-Space-Commercialization-Strategic-Plan-6-pages.pdf>
- [4] White House (2010) National Space Policy of the United States of America (White House, Washington, D.C.) Available at https://obamawhitehouse.archives.gov/sites/default/files/national_space_policy_6-28-10.pdf
- [5] National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (National Institute of Standards and Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.04162018>
- [6] National Institute of Standards and Technology (2012) *Guide for Conducting Risk Assessments*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-30r1>
- [7] Committee on National Security Systems (2012) National Information Assurance Policy for Space Systems Used to Support National Security Missions (Committee on National Security Systems, National Security Agency, Ft. Meade, MD), Committee on National Security Systems Publication (CNSSP) No. 12. Available at <https://www.hsdl.org/?view&did=726945>
- [8] Federal Communications Commission (2021) *International Bureau Satellite Division*. Available at <https://www.fcc.gov/general/international-bureau-satellite-division>
- [9] INTENTIONALLY BLANK
- [10] “Land Remote Sensing Policy,” Title 51 *U.S. Code*, Subtitle VI, Chapter 601. 2010 ed. Available at

https://www.nesdis.noaa.gov/CRSRA/files/National_and_Commercial_Space_Programs_Act_60101.pdf

- [11] “15 CFR Part 960. Licensing of Private Land Remote-Sensing Space Systems; Final Rule.” 71 *Federal Register* 24474 (April 25, 2006), pp 24474-24491. Available at <https://www.nesdis.noaa.gov/CRSRA/files/15%20CFR%20Part%20960%20Regs%202006.pdf>
- [12] National Oceanic and Atmospheric Administration (2020) *About the Licensing of Private Remote Sensing Space Systems*. Available at <https://www.nesdis.noaa.gov/CRSRA/licenseHome.html>
- [13] Paganini P (2013) Hacking Satellites...Look Up to the Sky (Infosec Institute). Available at <https://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky>
- [14] Paganini P (2011) Hacking satellites. *Security Affairs*. Available at <http://securityaffairs.co/wordpress/236/cyber-crime/hacking-satellites.html>
- [15] Greenberg A (2010) How To Hack The Sky. *Forbes.com*. Available at <https://www.forbes.com/2010/02/02/hackers-cybercrime-cryptography-technology-security-satellite.html>

614 Appendix A—Examples of Relevant Regulations

615 This appendix provides examples of regulations that may be relevant to some but not all
616 commercial satellite operations. It is important for each organization to identify the potential
617 regulation and regulatory agency that applies to their specific operations and business.

618 DoD/IC/NGA

619 From the *National Information Assurance Policy for Space Systems Used to Support National*
620 *Security Missions* by the Committee on National Security Systems Publication (CNSSP) No. 12:

621 Presidential Policy Directive (PPD-4), *National Space Policy of the United States of*
622 *America*...reiterates that United States national security is critically dependent upon
623 space capabilities and this dependence will grow. Space activities are also closely linked
624 to the operation of the United States Government's (USG) critical infrastructures and
625 have increasingly been leveraged to satisfy national security requirements. Therefore,
626 increased assurance and resilience are needed for the mission-essential functions of
627 national security space systems, including their supporting infrastructure, to help protect
628 against disruption, degradation, and destruction, whether from environmental,
629 mechanical, electronic, or hostile means.

630 The primary objective of this policy [CNSSP-12] is to help ensure the success of national
631 security missions that use space systems, by fully integrating information assurance into
632 the planning, development, design, launch, sustained operation, and deactivation of those
633 space systems used to collect, generate, process, store, display, or transmit national
634 security information, as well as any supporting or related national security systems. Fully
635 addressing information assurance is especially important for the space platform portion of
636 space systems, since any vulnerability in them normally cannot be eliminated once
637 launched.

638 Federal Communications Commission (FCC)

639 Regarding the International Bureau Satellite Division, Federal Communications Commission
640 (FCC):

641 The primary mission of the Satellite Division is to serve U.S. consumers by promoting a
642 competitive and innovative domestic and global telecommunications marketplace. The
643 Division strives to achieve this goal by:

- 644 1. Authorizing as many satellite systems as possible and as quickly as possible to facilitate
645 deployment of satellite services;
- 646 2. Minimizing regulation and maximizing flexibility for satellite telecommunications
647 providers to meet customer needs;
- 648 3. Fostering efficient use of the radio frequency spectrum and orbital resources. The
649 Division also provides expertise about the commercial satellite industry in the domestic

650 spectrum management process and advocates U.S. satellite radiocommunication interests
651 in international coordinations and negotiations.

652 **Federal Aviation Administration (FAA)**

653 Regarding the Office of Commercial Space Transportation:

654 The Office of Commercial Space Transportation (AST) was established in 1984...as part
655 of the Office of the Secretary of Transportation within the Department of Transportation
656 (DOT). In November 1995, AST was transferred to the Federal Aviation Administration
657 (FAA) as the FAA's only space-related line of business. AST was established to:

- 658 • Regulate the U.S. commercial space transportation industry, to ensure compliance with
659 international obligations of the United States, and to protect the public health and safety,
660 safety of property, and national security and foreign policy interests of the United States;
- 661 • Encourage, facilitate, and promote commercial space launches and reentries by the
662 private sector;
- 663 • Recommend appropriate changes in Federal statutes, treaties, regulations, policies, plans,
664 and procedures; and
- 665 • Facilitate the strengthening and expansion of the United States space transportation
666 infrastructure.

667 **National Oceanic and Atmospheric Administration (NOAA)**

668 Regarding the Commercial Remote Sensing Regulatory Affairs (CRSRA) Licensing Program:

669 This web site is intended to provide U.S. laws, regulations, policies, and guidance
670 pertaining to the operation of commercial remote sensing satellite systems. Pursuant to
671 the National and Commercial Space Programs Act (NCSPA or Act), 51 U.S.C. § 60101,
672 et seq, responsibilities have been delegated from the Secretary of Commerce to the
673 Assistant Administrator for NOAA Satellite and Information Services (NOAA/NESDIS)
674 for the licensing of the operations of private space-based remote sensing systems.

675 In accordance with the Act, the regulations 15 CFR Part 960 concerning the licensing of
676 private remote sensing space systems have been promulgated.

677 Appendix B—Acronyms

678 Selected acronyms and abbreviations used in this paper are defined below.

679	AST	Office of Commercial Space Transportation
680	CFR	Code of Federal Regulations
681	CIO	Chief Information Officer
682	CNSS	Committee on National Security Systems
683	CNSSP	Committee on National Security Systems Publication
684	CRSRA	Commercial Remote Sensing Regulatory Affairs
685	CTO	Chief Technology Officer
686	DOT	Department of Transportation
687	FAA	Federal Aviation Administration
688	FCC	Federal Communications Commission
689	FOIA	Freedom of Information Act
690	IR	Internal Report
691	ITL	Information Technology Laboratory
692	LEO	Low Earth Orbit
693	NCSPA	National and Commercial Space Programs Act
694	NESDIS	National Environmental Satellite, Data, and Information Service
695	NIST	National Institute of Standards and Technology
696	NOAA	National Oceanic and Atmospheric Administration
697	OSC	Office of Space Commercialization
698	PPD	Presidential Policy Directive
699	SP	Special Publication
700	USG	United States Government

701 **Appendix C—Glossary**

702	Beacon	Initial signal by satellite conducted when first put into mission operation in order to establish communications with command and control and report initial operating status.
	BUS	Consists of the components of the vehicle associated with the “flying of the satellite,” such as power, structure, attitude control system, processing and command control, and telemetry. The spacecraft can carry many specialized payloads to conduct missions, including remote sensing and communications. The BUS and the payload generally combine to form the satellite.
	Payload	Mission-specific items of the overall satellite that are not part of the overall operations or “flying” of the satellite.
	Satellite	BUS and payload combined into one operational asset.
	Space Structures	Term referring to “space debris” or “space junk” that is no longer in use for any business or mission need.
	Umbilical Cord	Connective cabling to BUS, Satellite, Payload and/or Vehicle that can exchange data with the mission systems.
	Vehicle	Space-operational items that include the launching items that are used to place the satellite, BUS and/or payload into orbit.

703