CENTER FOR SPACE POLICY AND STRATEGY

OCTOBER 2021

POLICY COMPLIANCE ROADMAP FOR SMALL SATELLITES

ELENI M. SIMS, BARBARA M. BRAUN, AND AARON P. ZUCHERMAN
THE AEROSPACE CORPORATION

AEROSPACE

ELENI M. "SAM" SIMS

Eleni M. "Sam" Sims is a senior project engineer in The Aerospace Corporation's Space Innovation Directorate. For 24 years she has provided technical support to the Department of Defense (DOD) and currently works with the U.S. Space Force's Innovation and Prototyping Directorate. She has worked on science and technology programs as well as prototype programs, with an eye toward space access, mission design, and policy. Sims is an associate fellow with the American Institute of Aeronautics and Astronautics.

BARBARA M. BRAUN

Barbara M. Braun joined The Aerospace Corporation in 2000 and has supported multiple small satellite and rideshare missions for the Department of Defense Space Test Program, the Operationally Responsive Space Office, and NASA. She served in the Air Force for 21 years, both on active duty and in the reserves, where she worked on space safety policy for the Air Force Safety Center.

AARON P. ZUCHERMAN

Aaron P. Zucherman is a former graduate space policy intern at The Aerospace Corporation's Center for Space Policy and Strategy, where he supported research on space industry topics focusing on responsive space enterprises, leveraging commercial capabilities, modular and interoperable solutions, and the insertion of new and game-changing technologies and innovations into heritage organizations. His academic experience spans from mission management of Earth orbiting and interplanetary CubeSat missions, agile space technology development, risk and cost analysis, and applying systems engineering methodologies to the development of interplanetary small satellite missions. Zucherman is a Matthew Isakowitz Commercial Space Fellow and systems engineering Ph.D. candidate at Cornell University.

ABOUT THE CENTER FOR SPACE POLICY AND STRATEGY

The Center for Space Policy and Strategy is dedicated to shaping the future by providing nonpartisan research and strategic analysis to decisionmakers. The center is part of The Aerospace Corporation, a nonprofit organization that advises the government on complex space enterprise and systems engineering problems.

Contact us at www.aerospace.org/policy or policy@aero.org

AEROSPACE

Summary

This paper explores United States (U.S.) space policies and how they apply to satellite missions that may not fit the typical satellite mission mold. The paper presents a "roadmap" for policy compliance for satellites from diverse agencies and identifies areas where further work is underway to address the challenges posed by the evolution of the space industry. The paper lays out a coherent way forward for all small satellites navigating the approval quagmire, and for mission managers of multi-payload rideshares who wish to smooth the path to launch approval.

Introduction

In the early days of satellite development and launch, only governments or government contractors built satellites and rockets, and generally each launch carried only a single satellite to orbit. Today, the space enterprise encompasses many players and stakeholders, including small businesses, universities, affinity organizations, and even primary schools. The proliferation of small satellites (or "smallsats") has led not only to large numbers of new entrants into the space business, but also to an increasing number of rideshares, and the paradigm of a single launch carrying a single mission to space is no longer the norm.

The Aerospace Corporation supports a diverse customer base and has insight into policy issues across multiple agencies and departments, which allows us to understand policy applicability and to identify where policy "boundaries" exist. In this white paper, we explore U.S. space policies and how they apply to satellite missions that may not fit the "typical" satellite mission mold, on launch missions that may not have a single responsible agency. Where applicable, we have outlined the processes and approvals involved in getting to space. In addition, we have identified where further work is required to fill in policy gaps and "gray areas" in the overall policy picture.

Like the space industry itself, policy is constantly evolving. While we have tried to capture the current "policy roadmap" as accurately as possible, we welcome corrections and updates from the community as the picture comes into better focus.

Policy Overview

International Treaties and U.S. National Policy

The Outer Space Treaty of 1967 forms the basis of international space law, and stipulates that the signatories "shall be responsible for national space activities whether carried out by governmental or non-governmental agencies."[1,2] It places the responsibility for operations in space on the government of the nations that fly in space and requires "authorization and continuing supervision" by that government. In the Outer Space Treaty, a nation "on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such object…." This implies that the U.S. government has responsibility over U.S.-owned objects in space, regardless of whether that object is launched by the U.S. or by a foreign launch provider. Similarly, foreign satellites remain the property of foreign entities, even if launched from a U.S. rocket. While the Outer Space Treaty places joint liability for damage on the country "from whose territory or facility a space object is launched" as well as the country that procured the launch, this liability is only absolute for damages on Earth and to aircraft in flight. For damages in space, the launching country shall be liable "only if damage is due to its fault or the fault of persons for whom it is responsible"—in other words, only if the damage is due to the launching country's negligence or malicious intent.

Within the U.S., National Space Policy[3] also directs safe and responsible operations in space. Specific sections discuss protection of the space environment (including debris mitigation) and protection of the electromagnetic spectrum. The National Space Policy also discusses cybersecurity for U.S. space systems, which flows into lower-level guidance on cryptographic protection of space systems. Similarly, the National Space Transportation Policy[4] outlines the authorities for military, civil, and commercial launch oversight. Military oversight is provided by the Department of Defense (DOD); civil oversight is provided by the National Aeronautics and Space Administration (NASA). Commercial space transportation oversight is under the Secretary of Transportation; thus, commercial launches are licensed by the Federal Aviation Administration (FAA). These policies are often subject to change and reinterpretation based on current U.S. political leadership.

The Responsibilities of the Launch Provider Versus Satellite Owner

The National Space Transportation Policy, true to its name, discusses mainly access to space in the form of launches rather than operations in space once satellites have separated from the launch vehicle. Similarly, most of the lower-level policies demarcate the responsibilities of the launch provider and the responsibility of the spacecraft owner/operator at the point where the spacecraft separates from the launch vehicle or its upper stage.

In other words, the launching agency is responsible for launch policy, and is generally not the policy gatekeeper for the satellites it launches. Without the ability or authority to enforce policy throughout the satellite's orbital lifetime, the launching agency cannot ensure compliance. Instead, compliance must be enforced through the parent agency of the satellite owner/operator. Thus, a NASA satellite launched on a DOD rocket must demonstrate compliance with NASA policy, not DOD policy. Similarly, a DOD satellite on a commercial launch must still demonstrate compliance with DOD policy, not commercial policy. Figure 1 illustrates the general responsibilities of mission partners on a launch mission, and Figure 2 illustrates in more detail how these policy responsibilities break down for a sample multi-payload mission.

While this demarcation provides a convenient boundary for separating the responsibility of the launching agency from the responsibility of the satellite provider, in practice the line is less clear-cut. Recent events[5] illustrate the hazards of a launch provider leaving regulatory compliance entirely up to the satellite provider. Even though, once launched, these satellites are no longer necessarily under the authority or direction of the launching agency, U.S. launch providers have a strong incentive to ensure all pre-launch approvals are in place. Most launch providers now require documentation of policy compliance before satellites are integrated for launch. It is important at the beginning of a mission to clarify this demarcation and the proper policy compliance responsibilities for all satellite provider partners. The launching agency may still "refuse service" to a

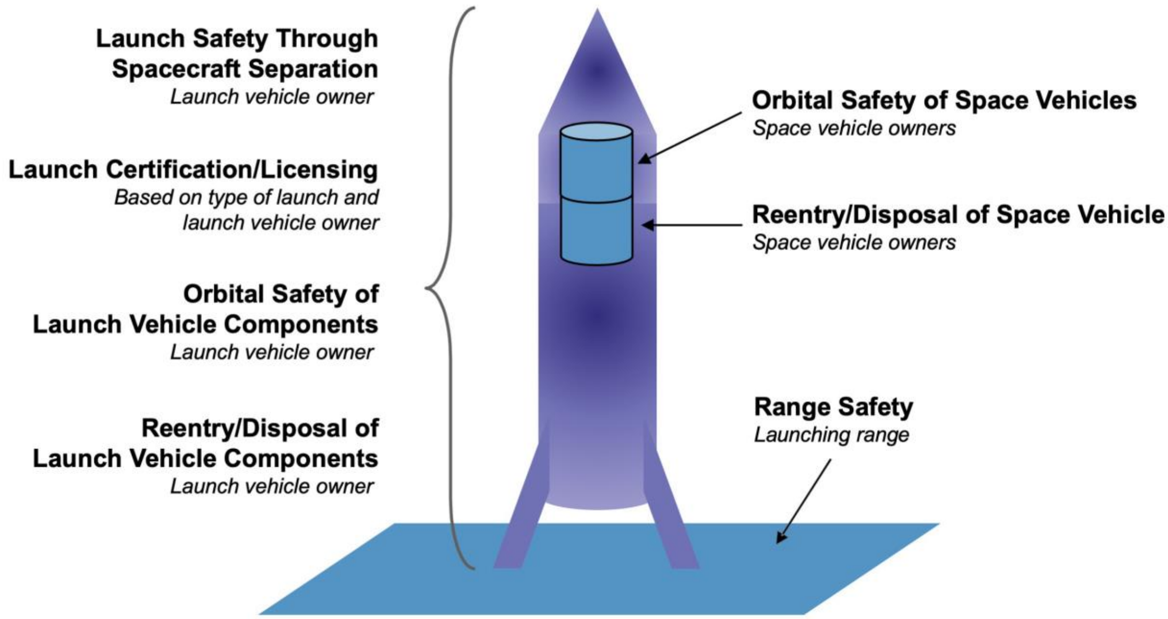

Figure 1: Policy compliance and safety responsibilities for launch missions.

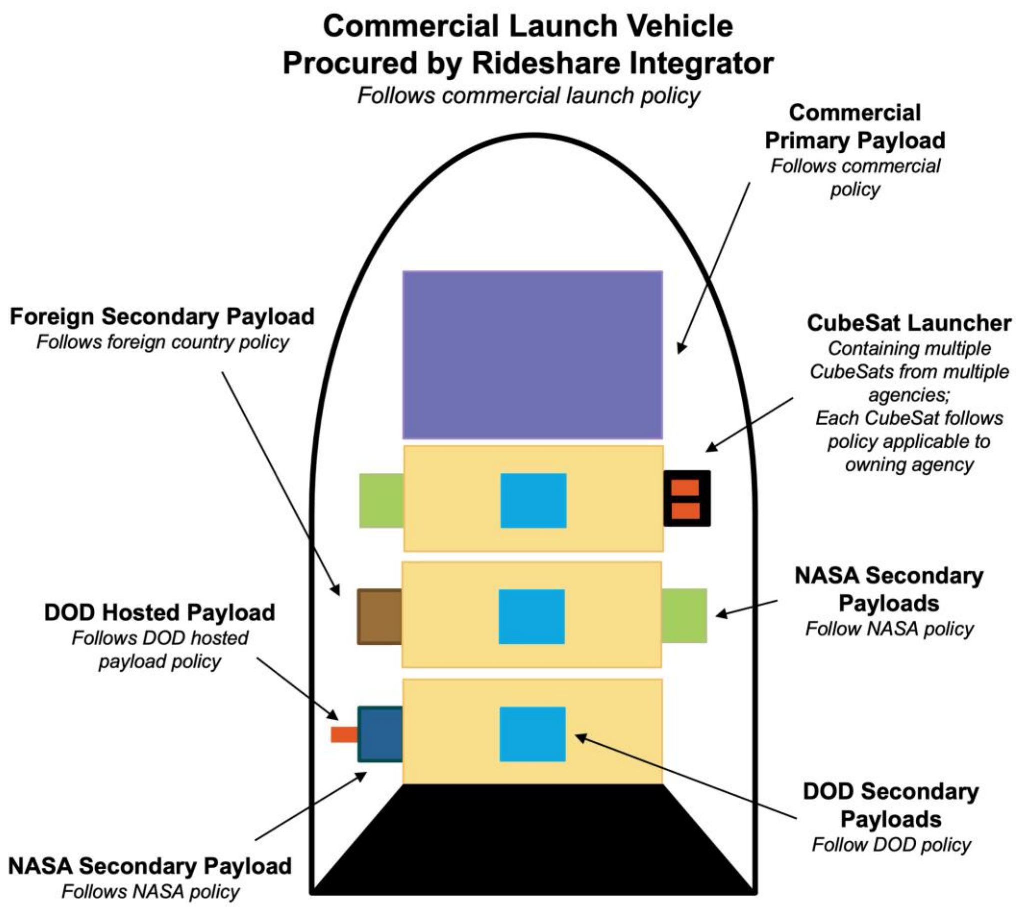

Figure 2: Rideshare policy compliance for multiple payloads.

satellite that does not meet certain requirements, even if those stipulations are not required by policy.

Special Consideration for Foreign Launch of U.S. Government Small Satellites

The emergence of new launch providers for small satellites has led to questions about the suitability of these launch providers for U.S. government missions. Many of these launch providers are subsidiaries of foreign companies or maintain launch sites in foreign countries. Because there is a body of policy and law that requires U.S. government satellites to be launched on U.S. launch providers, a determination specifically for these companies is required.

Several U.S. law and policy statements require launch vehicles for U.S. government satellites to be manufactured in the U.S.[6,7,8] These laws and policy statements establish a two-part test to determine if a launch vehicle is manufactured in the U.S. and thus allowed to launch U.S. government satellites. The two tests are:

1. Is the launch vehicle company more than 50 percent owned by U.S. nationals? (Required by Title 51 of U.S. Code and Department of Defense Instruction 3100.12)

2. Are 50 percent or more of the launch vehicle components, by cost, manufactured in the U.S.? (Required by Title 41 of U.S. Code and the National Space Transportation Policy)

Most government launch agreements are also subject to the Federal Acquisition Regulations (https://www.acquisition.gov/browse/index/far). Part 52.225-18 of the Federal Acquisition Regulations also defines the "place of manufacture" as "the place where an end product is assembled out of components." This language appears to establish a third test to determine if a launch vehicle is manufactured in the U.S.: Namely, is the end product assembled out of components in the U.S.? However, in August 2018, the Deputy Secretary of Defense issued a memo confirming that the two-part test is sufficient. The government typically buys a launch service (the delivery to orbit), not the launch vehicle itself. In these cases, the government does not take possession of the launch vehicle, and therefore the launch vehicle is not an "end product" as defined by the Federal Acquisition Regulations. Recently the DOD has launched several small satellites from emerging providers, using non-U.S. launch sites, provided that the emerging providers meet the two-part test.

The recently released 2020 National Space Policy does appear to give new direction on government technology demos or scientific payloads being allowed to fly on foreign launches possibly allowing these payloads to bypass the two-part test but it is too early to see how this change will be implemented.

What Constitutes Ownership?

Determining the parent agency of the satellite is critical to understanding the applicability of U.S. space policy. The flowchart shown in Figure 3, developed in partnership with the DOD Space Test Program (STP) and Air Force Research Laboratory (AFRL), illustrates a method for determining satellite ownership. The key consideration is: "Who will have control authority over the satellite (or payload) once it launches?" Another, more direct, way to ask the question is: "Who has the authority to decide when to execute the satellite's end of life or deorbit procedure?" If the DOD makes the decisions for all critical spacecraft activities after launch (commonly referred to as Satellite Control Authority), then it is a DOD satellite, regardless of whether it is built or operated by a private company. Similar rules apply to NASA satellites, with the additional stipulation that NASA contracts and NASA grant recipients are also considered NASA satellites.

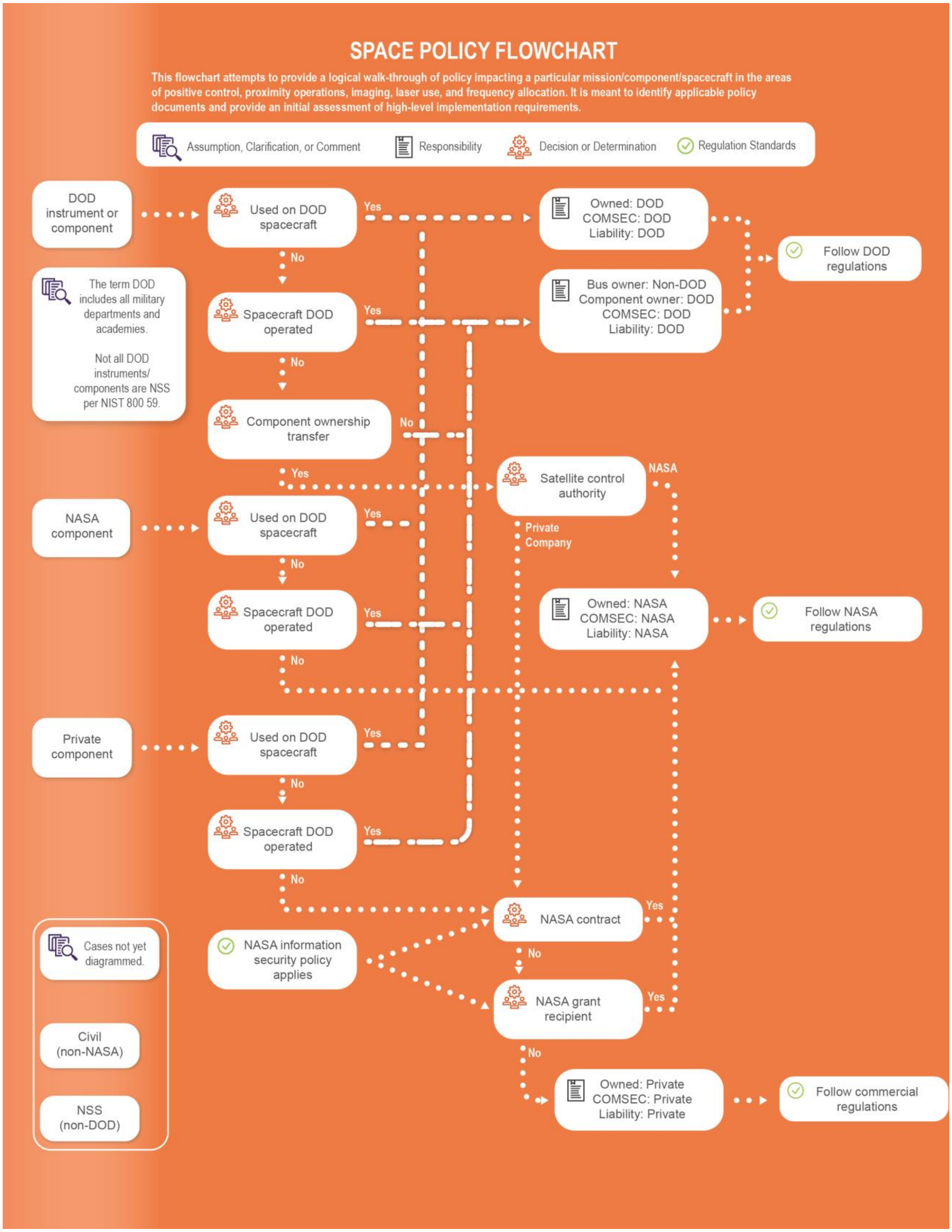

Figure 3: Flowchart for determining space vehicle ownership.

Some satellites, however, still fall into gray areas. For example, STP frequently arranges for the launch of private university or small business satellites sponsored to the DOD Space Experiments Review Board by military sponsoring agencies. Some of these university or small business satellites also receive small grants from the DOD. Although sponsored by the DOD, ownership of the vehicle and Satellite Control Authority remain with the universities. These organizations are private entities, and therefore such payloads currently follow a commercial path to comply with policy regulations, not a DOD path.

There are other "special cases," such as civil government satellites that are non-DOD, non-NASA satellites. Later sections will also discuss the special case of DOD satellites that are not National Security Space satellites, as these highlight other policy gray areas that require further clarification. However, sometimes gray areas also provide policy and decisionmakers with sufficient option space to accommodate new types of mission.

Once the owning organization is identified, the appropriate policies can also be identified. The DOD, NASA, the FAA, and the Federal Communications Commission (FCC) all have broad policy directives that flow down from the National Space Policy; these will be discussed in more detail in the applicable sections of this paper. We will discuss orbital debris mitigation policy, frequency allocation and spectrum usage, optical communications, information assurance, imaging, and rendezvous and proximity operations (RPO). We will also briefly discuss cislunar and interplanetary policy as it applies to small satellites.

Orbital Debris Policy

National Policy

As described above, the U.S. National Space Policy calls for protection of the space environment from orbital debris. Specifically, one of the "Cross-sector Guidelines" directs compliance with U.S. *Orbital Debris Mitigation Standard Practices* (ODMSP)[9] and requires "the head of the sponsoring department or agency" for space missions to approve exceptions.

The ODMSP are codified in a formal document that was updated in November 2019. The updated document begins with a preamble that provides an overview of the updates and discusses the motivation behind them. The first four technical sections govern debris generation, accidental explosion, minimizing the risk of collision with other objects, and disposal of space objects at the end of mission life. A new, fifth section discusses special cases of space operations, including large constellations, small satellites, rendezvous and proximity operations, active debris removal, and tether systems.

The ODMSP is the source of most of the debris requirements familiar to experienced satellite developers: the requirement for disposal within 25 years of the end of the mission, the requirement that reentering space objects not cause casualties on the Earth, and the requirements that limit the potential for in-space collision, debris generation, and accidental explosion. The 2019 update adds several numerical guidelines to the general recommendations, including a 1-in-1000 limit on the probability of accidental explosion, a 1-in-1,000 limit on the lifetime probability of collision with objects greater than 1 cm, and a 1-in-100 limit on the lifetime probability of collisions with objects less than 1 cm that could interfere with post-mission disposal. The new ODMSP also provide extensive guidance on post-mission disposal options and orbits and include a stipulation that any post-mission disposal maneuvers have at least a 90 percent chance of success. The 25-year time limit on atmospheric reentry is unchanged, but the new ODMSP encourages small satellites in particular to have orbital lifetimes "as short as practicable." The new, fifth section of the ODMSP specifically calls attention to constellations and small satellites (as well as tether systems, rendezvous and proximity operations, and active debris removal) but does not levy any additional requirements beyond those levied in the previous four sections.

Because these guidelines are national, they apply to all U.S. missions. Exceptions and waivers to the ODMSP typically require approval at very high levels and are increasingly difficult to get.

NASA Policy

NASA documents orbital debris mitigation requirements in *NASA Procedural Requirements for Limiting Orbital Debris* (NPR 8715.6B)[10] and *Process for Limiting Orbital Debris* (NASA-STD-8719.14A).[11] In this last document we find specific numeric limits to the probability of in-space collision, which mirror those included in the 2019 ODMSP. The document lists other detailed requirements for compliance with ODMSP and requires documentation of compliance in an *Orbital Debris Assessment Report* and an *End of Mission Plan*. Both the Report and Plan are approved through NASA channels, and exceptions flow up through the NASA Office of Safety and Mission Assurance. It is worth noting that the National Oceanic and Atmospheric Administration (NOAA) satellites also follow NASA Debris Mitigation Requirements.[12]

NASA has also recently issued two documents governing conjunction assessment and collision avoidance. NASA Interim Directive 7120.132, *Collision Avoidance for Space Environment Protection,*[13] outlines procedures for assessing and responding to the conjunction risk posed by debris and other space objects. It asks missions to document their collision avoidance practices in an *Orbital Collision Avoidance Plan*, and for the first time provides guidance on thresholds for collision avoidance, suggesting teams maneuver at a probability of collision threshold of 1×10^{-4} (one in ten thousand). NASA has also released a *Spacecraft Conjunction Assessment and Collision Avoidance Best Practices Handbook,*[14] which provides high-level guidance to missions.

Ambiguity, Open Questions, and Recommendations

Orbital Debris

The guidelines in the ODMSP represent one of the more well-known and universally accepted aspects of space policy, but policy gaps still exist. One of the biggest open questions is whether the FCC, whose mission typically has little to do with space, should be the agency to enforce orbital debris mitigation policy on the burgeoning commercial and private satellite business.

Several items in the FCC's recent *Further Notice of Proposed Rulemaking* are concerning to developers of small satellites. Small satellites and CubeSats typically lack robust propulsion systems; requiring all missions above 400 km to be capable of collision avoidance maneuvers would drive significant design changes with little benefit to the debris environment—and perhaps with unforeseen negative consequences. Small satellites also lack robust security and command authentication systems. The proliferation of CubeSats with propulsion but no encryption could pose a security concern. From a research and innovation perspective, requiring satellites to provide insurance, indemnification, or bonds against successful disposal will eliminate many academic programs that do not have the budget to do so. The lack of specific requirements for orbiting upper stages for non-DOD or NASA launches is a gap that policymakers must ultimately address.

Finally, many organizations lack specific policy guidance outlining the document format and approval authorities for orbital debris compliance. This can lead to confusion and ad hoc approaches to compliance, in an area where clarity is badly needed.[15]

FCC Policy

Private satellites—defined in this case as any satellite not owned or operated by NASA, NOAA, or the DOD—do not fall under any of the NASA and DOD policies, but must still comply with national orbital debris mitigation guidelines. This compliance is currently enforced by the FCC, through its licensing of uplink and downlink frequencies. Title 47 of the Code of Federal Regulations[18] requires applicants for frequency licenses to provide information on their orbits and their plans for orbital debris mitigation. FCC regulations also require the use of disposal options and the safe management of pressure vessels at the end of life. An examination of online documents shows that many private satellites, when applying to the FCC, use NASA's *Orbital Debris Assessment Report* format to document their orbital debris mitigation compliance.[19,20,21]

In October of 2018, the FCC provided a *Notice of Proposed Rulemaking* related to orbital debris, outlining several new potential changes to the FCC's regulations.[22] Many of the potential changes mirror the new ODMSP, but new rules requiring maneuverability above a certain altitude in low Earth orbit (LEO) and a performance bond for successful disposal were also proposed. Following a period of comment and review, the FCC published a final set of rules on August 25, 2020, and deferred some of the more contentious issues into a *Further Notice of Proposed Rulemaking*. The topics being tabled for further review include maneuverability above a certain altitude in LEO, post-mission orbital lifetime, indemnification, and the requirement for a performance bond for successful disposal. As of the writing of this paper, the FCC is reviewing comments from the *Further Notice of Proposed Rulemaking* and will be deciding what to do.

FAA Policy

The FAA licenses launch and reentry operations for non-government launches from U.S. soil or conducted by U.S. companies or citizens. Contrary to popular belief, it does not currently oversee or regulate satellites or activities in space. FAA regulations levy safety requirements on launch vehicles, including limiting the potential for debris generation and accidental explosions, and for reentry vehicles, limiting the potential for human casualties on the ground. The FAA, however, does not regulate the disposal of orbiting upper stages.[23]

Policy Compliance Process

Once the owning/operating agency for a satellite is known (see Figure 3), that agency must demonstrate compliance with its parent agency's orbital debris mitigation policy. For NASA, this involves the preparation and submittal of a *Space Debris Assessment Report* and *End of Mission Plan* in accordance with the NASA *Process for Limiting Orbital Debris*. The process is similar for Air Force missions, which complete an *Orbital Debris Assessment Report/End of Life Plan* in accordance with Air Force Instruction 91-202. Missions without defined processes or formats for debris compliance should consider using the NASA *Orbital Debris Assessment Report* as the template for demonstrating compliance with higher policy. This seems to be the practice for private satellites when requesting licenses from the FCC. Launch vehicles should follow the FAA process through the "end of launch," defined by the FAA as the last exercise of control over the launch vehicle. It is important to note that exceptions to *Orbital Debris Mitigation Standard Practice* guidelines require approval at very high levels: the head of the sponsoring department or agency. Such waivers are increasingly difficult and time-consuming to get, suggesting that satellite missions should conduct the required analyses early to allow time for design changes or waiver approvals, as needed.

Spectrum Usage

Summary of Applicable Policy

Public law and regulations, rather than policy, provide all guidance for the assignment and usage of spectrum for satellites. The National Telecommunications and Information Administration (NTIA) regulates frequency usage for federal agencies such as NASA and the DOD. The NTIA documents their rules and procedures in the *Manual of Regulations and Procedures for Federal Radio Frequency Management.*[24]

Through Title 47, the FCC licenses frequency use for non-federal agencies, including private and commercial satellites. Part 25 contains information about commercial and remote-sensing satellite communications, Part 5 covers experimental missions, and Part 97 covers amateur communications.[25]

Additionally, the International Telecommunication Union is the United Nations Specialized Agency responsible for telecommunications. The International Telecommunication Union does not have any authority to enforce policy, but the participating United Nations countries honor its treaty status. The International Telecommunication Union has its own rules and regulations codified in *Radio Regulations.*[26]

Policy Compliance Process

The NTIA is located within the Department of Commerce and is the agency responsible for managing the federal use of spectrum. Instructions for filing are laid out in the *Manual of Regulations and Procedures for Federal Radio Frequency Management*. The NTIA does not grant a frequency license, but instead grants the authority to use a frequency. The Frequency Assignment Subcommittee, within the NTIA, coordinates and assigns radio frequencies. NASA programs work their submission through the individual center spectrum management office and then the NASA spectrum management office. The NASA spectrum management office will then submit paperwork to the NTIA. DOD-owned missions submit through service-level spectrum management offices, who then submit to the NTIA.

There are four filing stages for federal programs: 1) Conceptual; 2) Experimental; 3) Developmental; and 4) Operational. Each is explained in detail in section 10.4.1 of the NTIA manual. Most small satellites performing science and technology, or research and development, missions will obtain a Stage 2 experimental license. Unlike the FCC, there is no requirement to conduct debris or lifetime analysis when applying to the NTIA.

The FCC is an independent U.S. government agency (overseen by Congress) that regulates interstate and international communications by radio, television, wire, satellite, and cable in the U.S. Part 25 of *Code of Federal Regulations Title 47: Telecommunications* outlines the application and filing process. Most small satellites will submit for either an amateur or an experimental frequency. The main difference is that amateur frequencies are for communications only, and the operator cannot have a financial interest on behalf of an employer. Experimental frequencies are, logically, for conducting experiments.

To use amateur frequencies, missions do not apply for a license for the satellite, but a licensed amateur operator must submit a pre-launch notification. Missions can submit an amateur filing by mail or by email. Additionally, for any use of amateur frequencies, missions must coordinate with the International Amateur Radio Union (IRU) and include that information with the package to the FCC. For an experimental license, the FCC requires that missions file electronically through their online tool. In both instances the FCC suggests that missions file no later than 30 days after the launch has been identified.

Ambiguity, Open Questions, and Recommendations

Spectrum Usage

There is strict protection of the amateur frequencies from use by experimental or federal programs. This has led to some confusion in the community as to the ability to use amateur bands, particularly since (until recently), experimental or federally-connected programs regularly used amateur bands. Missions, especially those run by service academies, who have previously used amateur bands are now having to determine whether to go through the FCC for an experimental frequency or through the NTIA.

Additionally, there is often confusion for programs that fall into "gray areas." For example, a university-owned and -operated satellite that receives funding from the DOD and launches on a DOD launch vehicle remains a private satellite, but is sometimes directed to the NTIA for frequency approval. Occasionally, missions get different answers from the FCC and the NTIA. The future will probably bring more of these "gray area" missions, and it would be helpful to have a single office for frequency submittals. That office could then route the approvals to either the NTIA or the FCC, as appropriate to each mission.

Since the FCC updated its rules, the FCC does not specifically refer to ODMSP, though FCC rules still follow the ODMSP all but in name. Theoretically, there could be a regulatory mismatch between the ODMSP and the FCC rules, which could lead to loopholes or gray areas in debris mitigation requirements. If a satellite also must obtain a NOAA imaging license, which still requires compliance with ODMSP, there could be further confusion as to what debris mitigation requirements apply, and who provides approval.

Missions filing with the FCC must demonstrate compliance with the debris mitigation guidelines (CFR 47 25.114d(14)), as described in the orbital debris section of this paper, and with other requirements specified by the FCC that go beyond the ODMSP. Missions must show that they adhere to debris generation guidelines, that they will deorbit within 25 years of end of life or move to a disposal orbit, and that they will not have an expectation of casualty other than zero when reentering. If missions cannot demonstrate this satisfactorily to the FCC, they may be required to carry insurance or risk not being approved to broadcast.

When frequency usage is approved, the FCC and NTIA submit their frequency assignments to an FCC liaison who then submits the U.S.'s assignments to the International Telecommunications Union who maintains the international register. Getting a license or approval to use a frequency through either agency takes months to years, so missions should start working on the application and submittal as early as possible.

Optical Communication (Lasercom)

Summary of Applicable Policy

Free-space optical (FSO) communication refers to the transmission of modulated light pulses through free space (vacuum or the atmosphere) to wirelessly transmit data for telecommunications or computer networking. Communication may be fully in space (an inter-satellite link) or in a ground-to-satellite or satellite-to-ground application. For satellite missions, the use of lasers for communication is often referred to as "lasercom" and has been increasing in popularity both due to the potential for high bandwidth and due to the limited availability of radiofrequency spectrum allocation.[27]

Currently, FSO as a form of communication in the optical spectrum (typically considered >3THz) is not heavily regulated. The rationale is that emitters in the optical and near infrared band have extremely narrow beamwidth, and space is vast, so the potential for damage is low. Nevertheless, DOD and DOD-funded missions are required to clear space-based laser activities through the Laser

Clearinghouse (LCH) to ensure orbital assets are not negatively impacted by lasers. Additionally, visible and infrared lasers have great potential for damage to the human eye. In the U.S., the FAA regulates commercial terrestrial FSO links to prevent distraction or damage to the eyesight of airline pilots.

Commercial Use of Lasers

The FAA regulates terrestrial laser communications in the U.S. for commercial applications. Any FSO link transmitting through "navigable airspace" requires coordination with the FAA. The FAA will issue a Letter of Non-Objection if it is determined that the laser system in question either poses no hazard to aircraft or that all hazards have been adequately mitigated. Otherwise, there will be a Letter of Objection issued. *FAA Order Job Order (JO) 7400.2M: "Procedures for Handling Airspace Matters" Chapter 29*, contains policy, responsibilities, and guidelines for processing a "Notice of Proposed Outdoor Laser Operation(s)" and determining the potential effect of outdoor laser activities.[28] Compliance practices are based on ANSI standards Z136.1: *American National Standard for Safe Use of Lasers*[29] and ANSI Z136.6*: American National Standard for Safe Use of Lasers Outdoors*.[30]

The Laser Clearinghouse

To reduce the possibility of U.S. DOD laser projects accidentally damaging satellites, the LCH was established. The LCH is tasked with providing predictive avoidance analysis and deconfliction with U.S., allied satellites, and operations for projects that utilize lasers.

All DOD run or funded laser programs operating to, in, through, or from space or which are aimed above the horizon are required to coordinate operations with the LCH by DOD Instruction 3100.11, *Illumination of Objects in Space by Lasers*.[31] For non-DOD users, ANSI Z136.6 advises that lasers that have a divergence less than 10 μrad, or that exceed a peak irradiance greater than 1 W/cm^2 above 18 km (60,000 ft) in altitude above sea level, should contact U.S. Space Command regarding LCH screening. This screening is not required by law or policy but still has a high likelihood of being required by the FAA to obtain a Letter of Non-Objection.[32]

The first step in the LCH process is to submit the Laser Registration Form at the Laser Clearinghouse website (https://www.space-track.org/documentation#lch), which outlines all relevant laser parameters. The LCH then reviews the form and provides a risk determination analysis, which indicates whether the laser's operation poses a threat to satellites. If the laser system is found not to pose a threat, a waiver can be given by the LCH and no further coordination is required. The owner/operator of the laser communication system can operate freely but must re-register with the LCH annually.

A project that is not given a waiver is required to submit its planned laser sources, targets, and planned times of operation to the LCH. This process involves registration with Space-Track.org and using LCH-provided templates and software for the development of a deconfliction plan. A deconfliction approach is then selected and a plan developed under the guidelines of the LCH. Control measures for deconfliction may include human aircraft spotters, radar systems, automated laser shutters, and laser pointing restrictions. Plan approval may be contingent on a site visit. Once approved, the LCH provides an authorization letter to the mission.

The process of coordinating with the LCH can be quite lengthy and may take many months. Laser projects should establish contact with the LCH as early as possible to understand the process. It may be possible to reduce the negative impact of LCH restrictions by making smart decisions early in the design of the system.

Ambiguity, Open Questions, and Recommendations

Optical Communications

Laser communications are becoming increasingly popular for space-to-ground and space-to-space communications links, and many proliferated LEO constellations are implementing or considering laser communications links. The paradigm where each laser shot is individually coordinated and cleared with either the FAA or the LCH is unlikely to be scalable to proliferated laser communications. Owners may need to ensure their lasers are low enough power to be exempt or the coordination process may need to be automated. Future satellite systems may also need to ensure they are unlikely to be damaged by lasers beneath a certain power, as deconfliction will be cumbersome.

Policy guidelines may need to be negotiated between the FAA and LCH as space-to-ground communications systems become more common. The FAA traditionally deconflicts laser use only with airlines, and commercial providers are not required to coordinate with the LCH. In the future, the FAA may need to take on more responsibility for commercial laser communications to space. Alternatively, the FCC might ultimately decide to regulate the optical spectrum as it does the radiofrequency spectrum—though the regulation of the optical spectrum is likely to focus on the prevention of damage, rather than the deconfliction of frequencies.

Cybersecurity/Information Assurance

Summary of Applicable Policy

Cybersecurity policy for small spacecraft is defined in a complex and confusing menagerie of policy documents published by the DOD, the Committee on National Security Systems, the National Institute of Standards and Technology, and other organizations. For all spacecraft used by the DOD, a key document is DOD *Instruction 8581.01, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense.*[33] This instruction implements Committee on National Security Systems Policy No. 12, *Cybersecurity Policy for Space Systems Used to Support National Security Missions.*[34] To determine if an information system is considered National Security Space, there is National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System.*[35]

Policy Compliance Process

There are two primary areas of compliance associated with spacecraft cybersecurity policy (although this is not exhaustive). The first concerns protection of the spacecraft uplink and downlink (i.e., the requirement for encryption). The second concerns certification and accreditation requirements of the spacecraft as an information system (i.e., the requirement to receive an Authority to Operate). These will be covered in turn.

Encryption

For DOD-owned or controlled spacecraft, Instruction 8581.01 requires encryption of the uplink and downlink. This applies to all DOD satellites, including research and development spacecraft built by DOD laboratories or academic institutions. Selection and implementation of the cryptography used to meet requirements should be coordinated with the National Security Agency early in the design phase of every spacecraft program.

For non-DOD federal spacecraft (i.e., NASA), encryption is not strictly required. However, National Institute of Standards and Technology Special Publication 800-53 does apply, and the criticality and sensitivity of information transmitted may lead to selection of security controls that include encryption.[36] Organizational policies may also apply. For example, NASA Procedural Requirements 2810.1A, *Security of Information*

Technology defines information technology security requirements for NASA.[37]

For commercial or private spacecraft, encryption is not typically required. However, if the DOD is *using* a commercial, private, non-DOD federal or foreign space system, DOD Instruction 8581.01 has requirements pertaining to encryption. Depending on the criticality and sensitivity of the DOD information being transmitted, uplink and/or downlink cryptography may be required ranging from National Security Agency-approved to commercial best practices.

To obtain a NOAA commercial remote sensing license, there are rigorous conditions to incorporate safeguards to ensure the integrity of system operations and security of its data. Early coordination with National Security Agency is recommended.

Certification and Accreditation

Instruction 8581.01 requires that all DOD-owned systems undergo cybersecurity accreditation in accordance with the Risk Management Framework.[38] A full discussion of the Risk Management Framework process is beyond the scope of this paper. However, two points are worth mentioning. Each DOD spacecraft program should determine who their cybersecurity Authorizing Official is early in the program. The Authorizing Official will ultimately issue the Authority to Operate for the spacecraft.

NASA *NPR 7120.5, NASA Space Flight Program and Project Management Requirements* requires a project protection plan based off threat summaries for NASA missions.[39] *NASA-STD-1006*, *Space System Protection Standard*, outlines baseline standards to improve space system protection from well-understood threats.[40] NASA maintains a list of candidate protection strategies that outlines best practices for programs. Programs each develop a Project Protection Plan that incorporates the results of the candidate protection strategy analysis, including any requisite requirement tailoring. NASA has a standard Project Protection Plan Template available.

Commercial spacecraft have no requirements to undertake a formal cybersecurity accreditation. When the DOD is using non-DOD systems, 8581.01 requires that the authorizing official for the DOD organization using the system perform a review of the space system's ability to meet cybersecurity requirements and accept the risk for any areas of noncompliance.

Ambiguity, Open Questions, and Recommendations

Cybersecurity/Information Assurance

The first ambiguity has to do with whether a spacecraft should be considered "DOD" and therefore subject to DOD cybersecurity policy. There have been differing interpretations received, with the most stringent classifying any spacecraft receiving DOD sponsorship or funding of any nature as DOD spacecraft and subject to all DOD policy requirements. This interpretation would have far-reaching implications and is not considered tenable. As described in the section on satellite ownership, satellites should be classified unambiguously and based on who is the owner/operator of the spacecraft. Cybersecurity policy compliance should be based on the requirements of the owner/operator organization.

A second ambiguity has to do with whether a satellite system is considered a National Security Space system. Not all DOD spacecraft are necessarily National Security Space systems. The National Institute of Standards and Technology Special Publication 800-59 has a checklist with six questions to determine if an information system is a National Security Space system. Based on this checklist, many DOD research and development spacecraft developed and operated by military laboratories and academic institutions are not National Security Space systems. As such, Committee on National Security Systems Special Publication No. 12 is not applicable. However, Department of Defense Instruction (DoDI) 8581.01 (which implements Committee on National Security Systems Special Publication No. 12) does not provide any provisions for non-National Security Space DOD spacecraft, which drives costly compliance requirements on these programs out of proportion to overall program cost and risk. DoDI 8581.01 should be revised to either explicitly exclude non-National Security Space DOD spacecraft or to provide streamlined compliance procedures for this class of spacecraft.

DoDI 8581.01 provides procedures for implementing cybersecurity when the DOD uses non-DOD spacecraft. However, "use" is not well-defined and subject to interpretation. It would be beneficial to expand this section of the policy to include different cases of "use" (such as hosted payloads, commercial imagery, and DOD sponsorship). Additionally, as hosting DOD payloads on non-DOD spacecraft becomes more common, cybersecurity requirements and responsibilities need to be better defined in memoranda of agreement up front.

Finally, there is no policy requiring the protection of non-DOD spacecraft command and control capability (particularly uplink encryption). This is of particular concern when the spacecraft has propulsion, or the ability to maneuver, because of the possibility of a "bad actor" gaining control of the vehicle and using it to interfere with another spacecraft. This is a significant policy hole that will become more pronounced with the increasing capabilities of small satellites and CubeSats, and especially if future FCC debris mitigation policy requires propulsion on satellites going to altitudes higher than 400km. Policy should be established requiring uplink security on all spacecraft with significant maneuver capability. This could be incorporated into the established process for securing an FCC frequency license. Federal organizations entering into agreements with foreign spacecraft should establish this requirement, particularly when the U.S. is providing launch services for the foreign spacecraft.

Imaging

Summary of Applicable Policy

Regulations governing remote sensing from a space platform fall into two distinct categories in the U.S.: Earth imaging and non-Earth imaging. There are also two types of satellites considered: commercial (civilian) satellites, and satellites owned and operated by the government. Satellites owned by DOD academic institutions are a considered a subtype of government-owned satellites and fall into their own unique policy bucket. This section will explore the various policies that apply to each type of satellite in each regulatory category and provide a basic understanding of how to navigate the policy compliance process.

Satellites owned and operated by commercial entities and civilian academic institutions are governed by the National Commercial and Space Programs Act.[41] This law governs Earth imaging and assigns authority to the NOAA for licensing of the same. For satellites owned by commercial and civilian academic institutions, NOAA will ensure all imagers also comply with DOD and intelligence community requirements for non-Earth imaging.

Government agencies currently have no requirement to obtain licensing for Earth imaging, although it is highly recommended that DOD agencies seek agency guidance. Non-Earth imaging for operational DOD systems is managed by the Defense Remote Sensing Working Group. Experimental DOD satellites are governed by interim guidance issued by the Principal DOD Space Advisor Staff.[42] This interim guidance, issued in 2015, requires DOD experimental satellites with remote sensing capability to submit test plans, data protection plans, and technical specifications of their system and payloads through the secretary of the Air Force Space Programs (SAF/AQS) office. If it is determined that a concern exists with respect to an experimental DOD satellite, the issue is automatically referred to the Defense Remote Sensing Working Group. Since this interim guidance was issued in 2015, there has been no effort to establish permanent policy or guidance. Imaging approval for DOD experimental satellites remains a gray area.

In researching this section, the team was unable to identify any NASA guidance or documentation with respect to imaging approval. All imaging devices aboard NASA satellites and missions are handled on a case by case basis by NASA.

Policy Compliance Process

The compliance process for commercial and civilian entities is outlined on the NOAA Commercial Remote Sensing Regulatory Affairs website. NOAA recommends beginning the process with informal, non-binding meetings between the applicant and the NOAA to help inform the process and prevent rework. When an organization is prepared to begin the application process, Code of Federal Regulations Title 15 Part 960 (amended in 2020) establishes the rules and procedures to be followed and the NOAA provides support to ensure all the required documentation is provided.[43] All license determinations are required to be made within 120 days of receipt of a completed application unless written guidance is provided on issues that exist with the application. All licenses are valid for the operational lifetime of the system unless voided through action of the owner or operator.

Ambiguity, Open Questions, and Recommendations

Imaging

Additional or clarifying guidance related to military academic institutions, satellites that receive DOD funding, and experimental satellites has not been established since the original publication of this paper in 2017 and remains an area open to interpretation.

Under the revised definitions in 15 CFR Part 960, remote sensing now applies only to imaging conducted when in orbit around the Earth (rather than in orbit of any celestial body) and to the collecting of data that can be processed into imagery of Earth surface features. NOAA licenses are not necessary for "instruments used primarily for mission assurance or other technical purposes, including but not limited to navigation, attitude control, monitoring spacecraft health, separation events, or payload deployments, such as traditional star trackers, sun sensors, and horizon sensors . . ." Additionally, if a spacecraft only has instruments incapable of producing data that can be processed into Earth-surface imagery, then they are not required to obtain a license.

The amended version adds a tiering system for applicants based on the availability of their unenhanced data from other sources. Tier 1 is for systems that are capable of only producing unenhanced data that is substantially the same as data available from other sources not regulated by the Department of Commerce (e.g., foreign sources) and will receive minimal license conditions. Tier 2 is for systems that can produce unenhanced data that is substantially the same available from U.S. sources. Tier 3 is for systems that produces data that has no competitors, foreign or domestic and may receive the more stringent license conditions.

Rendezvous and Proximity Operations

Summary of Applicable Policy

"Rendezvous and proximity operations" is a broad term used to describe any operations that intentionally take one satellite into the vicinity of another. Current proximity operations policy is a patchwork of policy and guidance documents across the space community. The 2019 update to the ODMSP for the first-time references rendezvous, proximity operations, and satellite servicing in its new Objective 5-3; programs are encouraged to limit the probability of accidental explosion resulting from the operations. Specific numeric thresholds for these guidelines, and definitions of what constitutes "proximity operations," however, have not yet appeared in lower-level guidance.

As the capability of small satellite systems increases, the desire for missions to perform proximity operations becomes more of a reality. Spacecraft designers must balance the need to perform mission objectives with safety of flight concerns—because of its debris-generating potential, a collision between two satellites is a concern for the entire space environment, not just the two satellites involved. Although not necessarily considered proximity operations, space safety concerns extend to formation flying missions which intend to maintain a constant relative distance to each other. NASA currently has no policy guidance concerning proximity operations. There is a policy in the DOD for the review of proximity operations missions, but this policy is not widely available. Neither the FCC nor the FAA has any policy compliance requirements for on-orbit proximity operations.

Policy Compliance Process

DOD missions intending to perform proximity operations missions must comply with DOD processes. Civil and commercial entities are currently not required to comply with any process specific to proximity operations objectives, although missions will naturally need to comply with all frequency and imaging requirements discussed above.

Ambiguity, Open Questions, and Recommendations

Rendezvous and Proximity Operations

With the growth in capability of small satellites there has been a surge in formation flying, rendezvous, proximity operations, and docking missions. Due to the technical challenges of performing these missions and the inherent safety of flight concerns, clarification on processes for civil and commercial entities would be beneficial. The policy should distinguish between formation flying and proximity operations and define policy guidance for each class. One possible definition for proximity operations might define proximity operations as satellites that deliberately operate within the typical screening volumes used for conjunction assessment, continuously for long periods of time. These vary but are on the order of 20 km in the along-track direction, and 1 km in the cross-track and radial directions. Missions that intend to approach other satellites or cooperatively fly within these distances might be required to develop proximity operations safety plans. It is recommended for both formation and proximity operations missions that mission designers comply with National Institute of Standards and Technology Special Publication 800-53 and implement commercial best practice encryption on the uplink and downlink.

A related issue that needs to be captured (possibly in this policy) involves cybersecurity requirements for vehicles with propulsion, regardless of their intention to conduct proximity operations. Key to this guidance should be directives based off the amount of propulsion (or "delta-V") that a space vehicle intends to carry. This should inform the cybersecurity posture of the vehicle and ground system. Care should be taken to separate policy requirements for significant translational propulsion systems from those required for simple attitude control propulsive systems.

Operations Beyond Earth Orbit

Summary of Applicable Policy

The number of launch opportunities for missions beyond Earth orbit are expected to grow in the coming years given NASA's renewed commitment to lunar exploration with the Artemis Program and a new generation of heavy and superheavy launch vehicles. Additionally, the proliferation of public and private exploration partnerships such as NASA's Commercial Lunar Payload Services program has the potential to involve commercial organizations that have never operated in this region of space before. Small satellites, traditionally confined to low Earth orbit, are increasingly being considered and used for missions beyond geosynchronous orbit.[44] This section briefly addresses policy related to operations beyond Earth orbit.

Imaging

In the newly amended CFR Title 15 Part 960, any NOAA-regulated spacecraft orbiting celestial bodies other than the Earth are not required to obtain a license even if containing instruments theoretically capable of producing Earth-surface imagery.

Planetary Protection

Article IX of the Outer Space Treaty states: "...parties to the Treaty shall … conduct exploration of [the Moon and other celestial bodies] so as to avoid their harmful contamination and also adverse changes in the environment of the Earth resulting from the introduction of extraterrestrial matter." The United Nations Committee on Space Research (COSPAR) maintains and promulgates the internationally accepted approaches to planetary protection on behalf of Article IX.

NASA's planetary protection requirements are founded upon COSPAR policy and fall under the Office of Planetary Protection.[45] All NASA launched or funded missions which might intentionally or unintentionally carry Earth organisms and organic constituents to other solar system bodies, or any mission employing spacecraft which are intended to return to Earth and/or its biosphere from extraterrestrial targets of exploration, must be compliant with NPD 8020.7, *Biological Contamination Control for Outbound and Inbound Planetary Spacecraft*.[46]

Protection requirements are specific to the type of mission and planetary bodies visited. As described in NPR 8020.12, *Planetary Protection Provisions for Robotic Extraterrestrial Missions*, missions must meet a certain set of forward contamination criteria that prevents unintended encounters with solar system objects and limits the probability of contamination if encounters are unavoidable. Missions to objects of interest for origins of life (including Earth's moon) require documentation of mission trajectory and disposition of hardware.[47] The NID 8715.128, *Planetary Protection Categorization for Robotic and Crewed Missions to the Earth's Moon,* addresses the control of forward biological contamination associated with all NASA and NASA-affiliated missions intended to land, orbit, or otherwise encounter the moon.[48] Additionally, NID 8715.129, *Biological Planetary Protection for Human Missions to Mars*, outlines requirements to avoid harmful forward and backward biological contamination under Article IX.[49]

Careful mission design and planning are essential elements when considering planetary protection requirements, and consultations with the planetary protection officer (PPO) during mission development is critical in ensuring compliance with NASA policy.

Ambiguity, Open Questions, and Recommendations

Beyond Earth Orbit Missions

As missions beyond Earth become more accessible to small satellites, policymakers will need to start regulating debris, particularly in lunar orbit and high-value areas such as Lagrange points. Orbits around or near Lagrange points may ultimately need to be subject to similar regulations as satellites in geosynchronous orbit, with specific slots assigned to ensure lack of dangerous interference. Additionally, orbits in the cislunar regime are subject to high perturbations and further study is needed to determine safe disposal options.[50]

To date, NASA is the only agency with any significant planetary protection expertise, and it does not regulate commercial activity. Agencies such as the FCC, FAA or the Department of Commerce may ultimately need to regulate planetary protection for commercial missions.

The DOD has issued no guidance to date on how it intends to comply with Article IX.

Note: For the oversight of non-NASA-run or -funded missions, the U.S. process is not yet well-established.

Debris Mitigation

The current ODMSP does not specifically address debris mitigation requirements in cislunar or interplanetary space. However, the Air Force is beginning to examine this question and is drafting guidance to extend basic debris mitigation requirements (limiting probability of explosion, avoiding disposal in high-value regimes, etc.) to cislunar space and beyond.

Policy "Flowchart" and Sample Walkthrough

Figures 3 through 6 summarize all the policy pathways described in this paper, to the extent that the authors understand the existing policy framework. Starting in Figure 3, above, missions must first determine who "owns" the satellite, in order to determine what policy applies. Typically, the ultimate satellite owner/operator—whoever will have satellite control authority once the satellite is operational—is the agency whose policy the mission must follow. Once the mission ownership is understood, the remaining figures (Figures 4 through 6) describe the applicable policy.

As an example, if AFRL builds a satellite intending to conduct unclassified proximity operations, the Air Force is the owner/operator, and the DOD policy flowchart should be followed. DOD satellites are required to abide by information assurance requirements as documented in DOD Instruction 8581.01, and even if the mission is unclassified, must use National Security Agency-approved encryption. Such a satellite would apply to the NTIA for frequency assignment. Since the satellite will perform proximity operations, DOD proximity operations regulations must be followed.

As another example, assume that a university builds a satellite capable of Tier 1 imaging and is planning to do RPO activities. They get a government organization to sponsor it to the DOD Space Experiments Review Board (SERB) for launch consideration. Even with government involvement, the satellite is still considered a private satellite and will follow public policy for privately owned satellites. It will apply for a frequency license through the FCC and apply to NOAA for imaging approval. As part of its FCC filing or through NOAA's imaging approval, it will demonstrate its compliance with one of the respective debris mitigation regulations. While the mission will have to submit a data protection plan to NOAA, as long as their imagery product does not need protecting, there are no existing regulations requiring such a satellite to encrypt its uplink or downlink, and no specific approvals needed related to RPO.

Recent Developments

The Small Satellite Coordination Activity (SSCA) is a DOD-level effort initiated by the Under Secretary of Defense for Acquisition and Sustainment, Ms. Ellen Lord, in 2018. The effort was started to better understand what was being done across the department in the area of small satellites. Since 2018, a group of representatives from across the DOD and NASA have met quarterly in order to better understand DOD small satellite efforts and where the challenges lie. So far, there have been three phases to the SSCA. The first phase (February 2018 to July 2018) focused on data collection, the second phase (August 2018 to February 2020) focused on road-mapping, and the third phase (February 2020 to September 2020) convened eight focus groups to study challenges and make recommendations. The eight focus groups were: launch, satellite vehicles, space operations and infrastructure, security, communications, remote sensing, navigation, and policy.

The policy focus group recommended including those with smallsat experience in space policy development and coordination to inform how policy impacts smallsat programs. Often, policy is written with large operational programs in mind and without insight into how certain decisions (or processes) impact smallsat programs. An additional recommendation was to develop training materials to help the smallsat program managers navigate policy processes. As discussed at length in this paper, it is often hard for program managers to understand what policies they must follow and how to comply. A final recommendation was the formation of a single office at the DOD level to act as an advocate for smallsat programs and assist with policy navigation. As of the writing of this paper, these recommendations are being coordinated through the department.

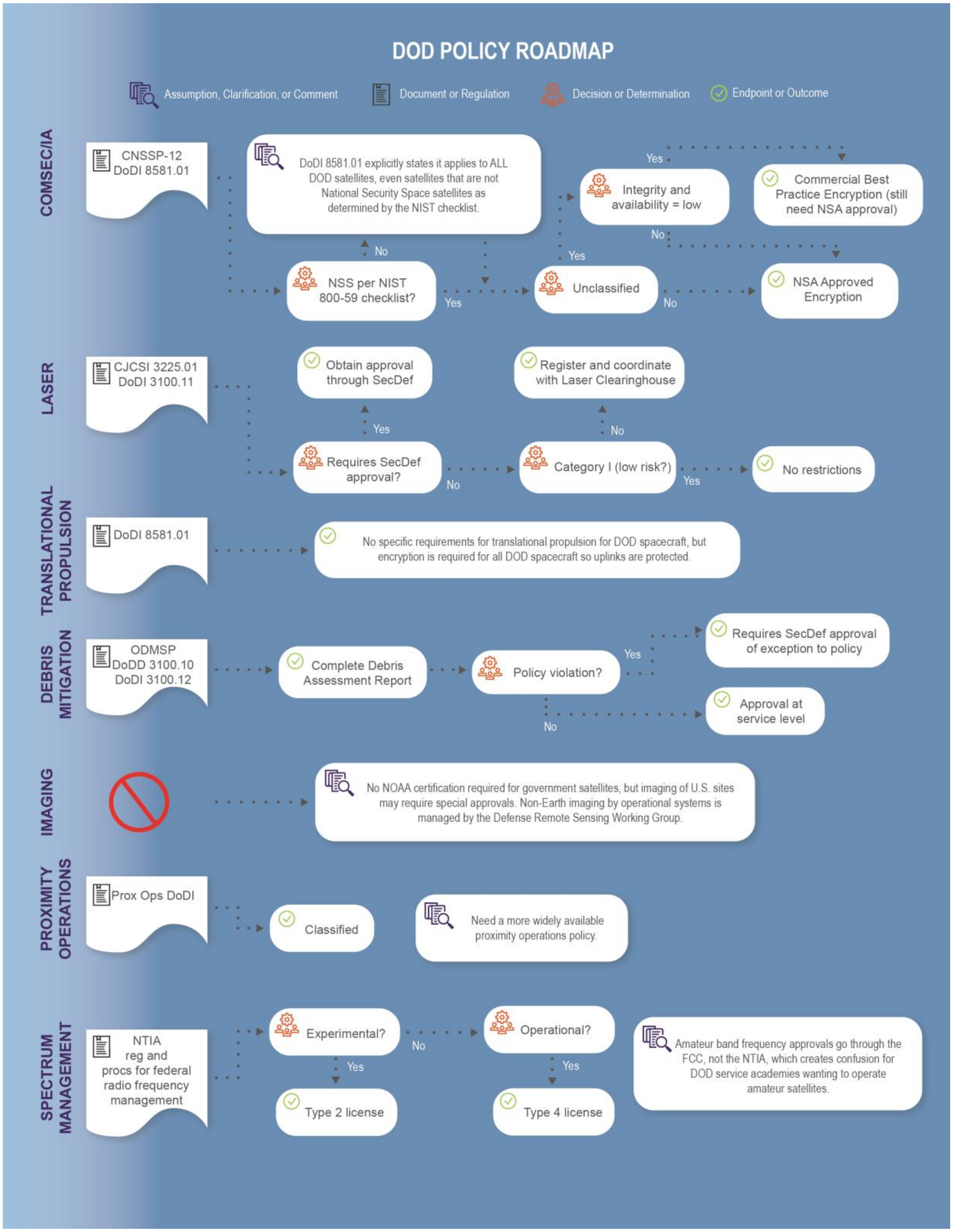

Figure 4: Policy roadmap for DOD satellites.

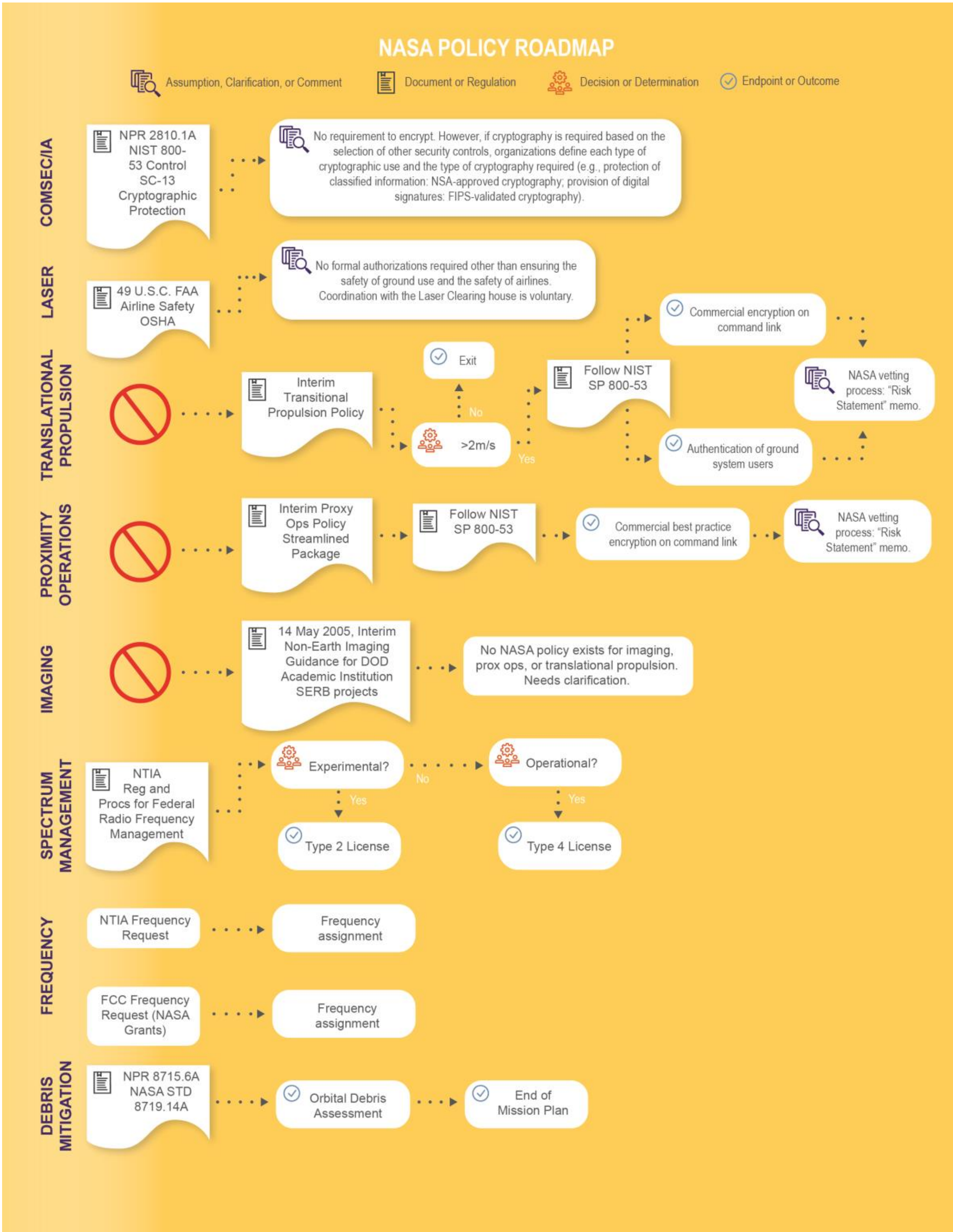

Figure 5: Policy roadmap for NASA satellites.

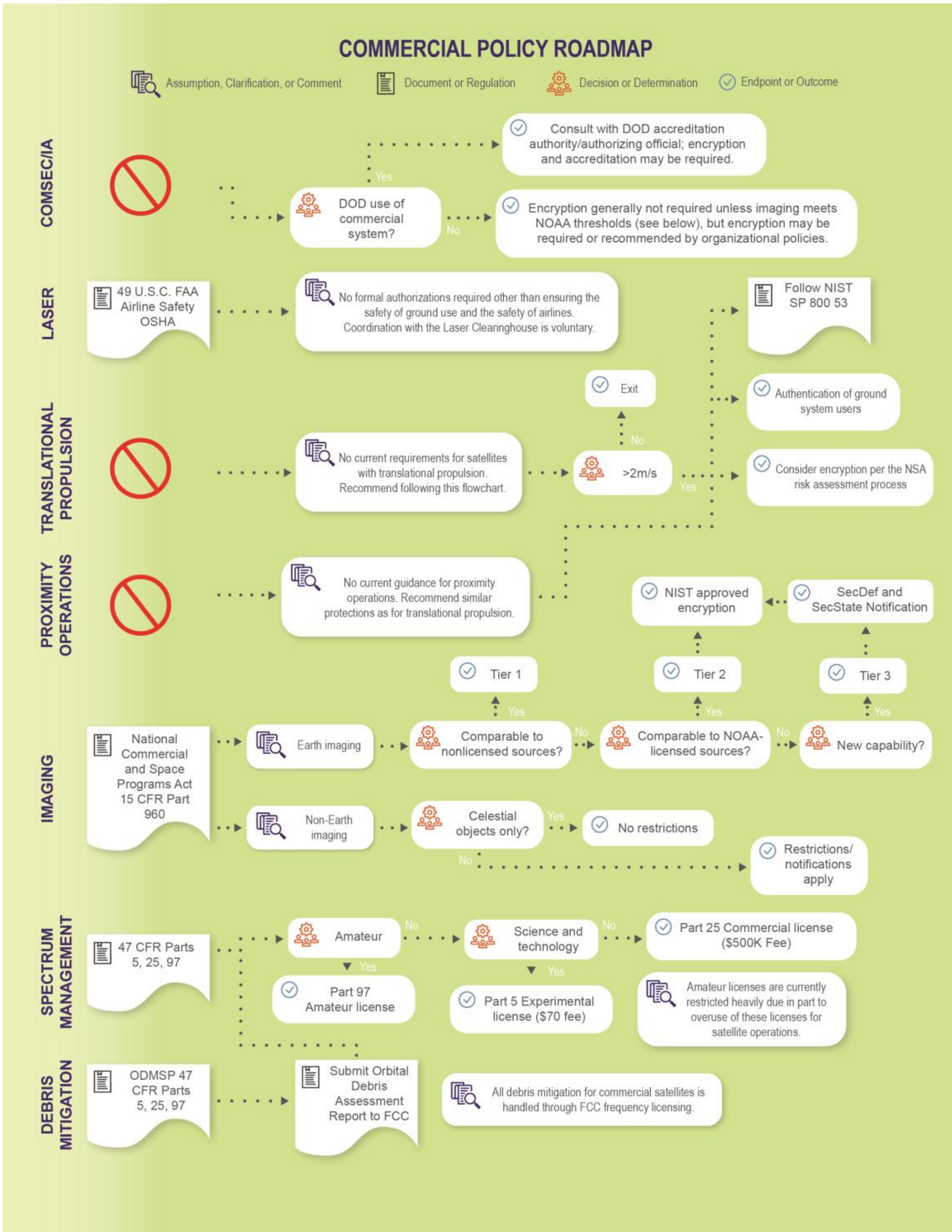

Figure 6: Policy roadmap for commercial satellites.

Conclusion

The policy picture for today's rapidly evolving space enterprise is complex and confusing, particularly to non-traditional entrants and missions that occupy policy "gray areas." In this paper, we have attempted to clarify the applicability of existing policy and outline a process for missions to follow to ensure compliance. We have also attempted to highlight areas where policy is absent or unclear. It is, however, important to remember that the policy roadmap is always "under construction," and that future changes are certainly expected. As of this writing, a new National Space Policy has been issued, and a new military service—the United States Space Force—has stood up. Policy roles and responsibilities are likely to evolve in response.

Acknowledgments

Transformation and re-engineering processes will require time, broad participation, and cooperation. However, the tempo of space launches is expected to increase with several large, new constellations on the horizon. Now is a propitious time to prepare for a more crowded and busy space environment. As the space enterprise evolves, we hope that U.S. policy will be agile enough to evolve with it, to ensure both access to space for all and safety in space for all.

The authors would like to acknowledge Ken Reese, David Butzin, Austin Potter and David Voss for their contributions to this effort.

References

[1] "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies," October 10, 1967, United Nations, New York, N.Y.

[2] "The Outer Space Treaty: Assessing Its Relevance at the 50-Year Mark," July 2017, James A. Vedda, The Aerospace Corporation (http://www.aerospace.org/publications/white-papers/the-outer-space-treaty-assessing-its-relevance-at-the-50-year-mark/).

[3] "National Space Policy of the United States of America," December 16, 2020, White House, Washington, D.C.

[4] "National Space Transportation Policy," November 21, 2013, White House, Washington, D.C.

[5] Braun, B., and Sims. E, "Trespassing on the Final Frontier: Regulatory Challenges for New Space Entrants," The Aerospace Corporation, June 2018

[6] Title 51, US Code, National and Commercial Space Programs, December 18, 2010 (http://uscode.house.gov/view.xhtml?path=/prelim@title51&edition=prelim).

[7] "Department of Defense Instruction 3100.12: Space Support." The Department of Defense, The U.S. Government, September 14, 2000 (http://www.au.af.mil/au/awc/awcgate/dod-spc/i310012p.pdf).

[8] Title 41, US Code, Public Contracts, January 4, 2011 (http://uscode.house.gov/view.xhtml?path=/prelim@title41&edition=prelim)

[9] "US Government Orbital Debris Mitigation Standard Practices, November 2019 Update," November 2019, The U.S. Government, Washington D.C., (https://orbitaldebris.jsc.nasa.gov/library/usg_orbital_debris_mitigation_standard_practices_november_2019.pdf).

[10] "NASA Procedural Requirements for Limiting Orbital Debris (NPR 8715.6A)," May 14, 2009, National Aeronautics and Space Administration, Washington, D.C.

[11] "NASA Process for Limiting Orbital Debris (NASA STD 8719.14A)," May 25, 2012, National Aeronautics and Space Administration, Washington, D.C.

[12] "Compendium of Space Debris Mitigation Standards Adopted by States and International Organizations," March 25, 2014, Committee on the Peaceful Uses of Outer Space, Vienna, Austria.

[13] "NASA Interim Directive 7120.132, *Collision Avoidance for Space Environment Protection*," November 2020, (https://nodis3.gsfc.nasa.gov/OPD_docs/NID_7120_132_.pdf).

[14] NASA *Spacecraft Conjunction Assessment and Collision Avoidance Best Practices Handbook*, December 2020 (https://nodis3.gsfc.nasa.gov/OCE_docs/OCE_50.pdf).

[15] Sorge, Marlon, "U.S. Space Debris Mitigation Regulatory Structure," The Aerospace Corporation, September 2017.

[16] "Department of Defense Directive 3100.10: Space Policy," October 18, 2012, Department of Defense, Washington, D.C.

[17] "Air Force Instruction 91-202: The US Air Force Mishap Prevention Program," June 24, 2015, Air Force, Washington, D.C.

[18] "Code of Federal Regulations Title 47: Telecommunications," April 19, 2016, Federal Communications Commission, Washington, D.C.

[19] "Dove 3 Orbital Debris Assessment Report," October 9, 2012, Cosmogia, San Francisco, CA.

[20] "Flock 1 Orbital Debris Assessment Report," June 20, 2013, Planet Labs, San Francisco, CA.

[21] "TechEdSat Formal Orbital Debris Assessment Report," April 2, 2012, NASA Ames, Moffett Field, CA.

[22] "Mitigation of Orbital Debris in the New Space Age," October 25, 2018, Notice of Proposed Rulemaking and Order on Reconsideration, IB Docket No. 18-313, Federal Communications Commission, Washington, D.C.

[23] "Space Debris Mitigation Policy," Fall 2015, Crosslink Magazine, The Aerospace Corporation, El Segundo, CA.

[24] "Manual of Regulations and Procedures for Federal Radio Frequency Management," May 2014, National Telecommunications and Information Administration, Washington, D.C.

[25] "Guidance on Obtaining Licenses for Small Satellites," March 15, 2013, Federal Communications Commission, Washington, D.C.

[26] "Radio Regulations," 2012, World Radiocommunication Conferences, International Telecommunication Union, Geneva, Switzerland.

[27] Sadiku, Matthew NO, Sarhan M. Musa, and Sudarshan R. Nelatury, "Free space optical communications: an overview," European scientific journal 12.9 (2016).

[28] "Procedures for Handling Airspace Matters," Job Order #7400.2M, Federal Aviation Administration, February 28, 2019 (https://www.faa.gov/documentLibrary/media/Order/7400.2M_Bsc_dtd_2-28-19.pdf).

[29] "American National Standard for Safe Use of Lasers," American National Standards Institute A136.1, 2014.
[30] "American National Standard for Safe Use of Lasers Outdoors," American National Standards Institute A136.6, 2015.
[31] "Department of Defense Instruction 3100.11: "Illumination of Objects in Space by Lasers," October 24, 2016, Department of Defense, Washington, D.C.
[32] Lafon, Robert, et al. "Regulatory Considerations: Laser Safety and the Emerging Technology of Laser Communication," American Institute of Aeronautics and Astronautics, *Space Operations: Experience, Mission Systems, and Advanced Concepts*, 2017.
[33] "Department of Defense Instruction 8581.01: Information Assurance Policy for Space Systems," June 8, 2010, Department of Defense, Washington, D.C.
[34] "Committee on National Security Space Policy No. 12: Cybersecurity Policy for Space Systems Used to Support National Security Missions," February 2018, Committee on National Security Systems, Ft Meade, MD.
[35] "National Institute of Standards and Technology Special Publication 800-59: Guideline for Identifying an Information System as a National Security System," August 2003, Department of Commerce, Washington, D.C.
[36] "National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, Department of Commerce, Washington, D.C.
[37] "NASA Procedural Requirements for Security of Information Technology (NPR 2810.1A)," May 16, 2006, National Aeronautics and Space Administration, Washington, D.C.
[38] "Risk Management Framework for Department of Defense Information Technology," March 12, 2014, Department of Defense, Washington, D.C.
[39] "NASA Space Flight Program and Project Management Requirements," NPR 7120.5, August 14, 2012, National Aeronautics and Space Administration, Washington, D.C.
[40] "Space System Protection Standard," NASA-STD-1006, November 5, 2020, National Aeronautics and Space Administration, Washington, D.C.
[41] "US Code Title 51: National Commercial and Space Programs," December 18, 2010, US Government Printing Office, Washington, D.C.
[42] "Interim Non-Earth Imaging Guidance for DoD Academic Institution SERB Projects," November 3, 2015, Department of Defense, Washington, D.C.
[43] "Code of Federal Regulations Title 15 Part 960," May 20, 2020, Department of Commerce, Washington, D.C.
[44] Freeman, A., 2020, "Exploring our solar system with CubeSats and SmallSats: the dawn of a new era," *CEAS Space Journal*, pp.1-12.
[45] Krage, J., "An Overview of NASA Space Protection" Presented to the Small Spacecraft Systems Virtual Institute (S3VI) Feb 2020.
[46] "Biological Contamination control for Outbound and Inbound Planetary Spacecraft," NPD 8020.7G, February 9, 1999, National Aeronautics and Space Administration, Washington, D.C. (https://nodis3.gsfc.nasa.gov/npg_img/N_PD_8020_007G_/N_PD_8020_007G__main.pdf).
[47] "Planetary Protection Provisions for Robotic Extraterrestrial Missions," NPR 8020.12D, April 20, 2011, National Aeronautics and Space Administration, Washington, D.C. (https://nodis3.gsfc.nasa.gov/npg_img/N_PR_8020_012D_/N_PR_8020_012D__Preface.pdf).
[48] "Planetary Protection Categorization for Robotic and Crewed Missions to the Earth's Moon," NID 8715.128, July 9, 2020, National Aeronautics and Space Administration, Washington, D.C. (https://nodis3.gsfc.nasa.gov/OPD_docs/NID_8715_128_.pdf).
[49] "Biological Planetary Protection for Human Missions to Mars," NID 8715.129, July 9, 2020, National Aeronautics and Space Administration, Washington, D.C, (https://nodis3.gsfc.nasa.gov/OPD_docs/NID_8715_129_.pdf).
[50] Cheney, Thomas, et al. "Planetary Protection in the New Space Era: Science and Governance." Frontiers in Astronomy and Space Sciences 7 (2020): 90.