CENTER FOR SPACE POLICY AND STRATEGY

NOVEMBER 2017

NAVIGATING THE POLICY COMPLIANCE ROADMAP FOR SMALL SATELLITES

ELENI M. SIMS, BARBARA M. BRAUN
THE AEROSPACE CORPORATION

ELENI M. SIMS

Eleni M. Sims is a project engineer in the Space Innovation Directorate. She provides technical support to the Air Force's Advanced Systems and Development Directorate—specifically the DoD Space Test Program—by architecting advanced science and technology missions. She is the lead technical support for three satellites on the STP-2 mission, which is scheduled to launch in early 2018.

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.

ABOUT THE CENTER FOR SPACE POLICY AND STRATEGY

The Center for Space Policy and Strategy is a specialized research branch within The Aerospace Corporation, a federally funded research and development center providing objective technical analysis for programs of national significance. Established in 2000 as a Center of Excellence for civil, commercial, and national security space and technology policy, the Center examines issues at the intersection of technology and policy and provides nonpartisan research for national decisionmakers.

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

Foreword

In the early days of the space age, only governments and their contractors built satellites and rockets, and each launch generally carried only a single spacecraft to orbit. Today, the space enterprise encompasses many players—not just governments and large corporations, but also small businesses, universities, and even high schools and affinity groups. The relative ease of developing small satellites has led not only to a large number of new entrants into the space arena, but also to an increasing number of rideshares, and the paradigm of "one launch, one mission" is no longer the norm.

The Aerospace Corporation supports a diverse customer base and works with multiple regulatory agencies to clarify applicable policy. This paper outlines U.S. space policies and explores how they apply to satellites that may not fit the typical mission mold and launches that may not have a single responsible agency. Where applicable, it outlines the processes and approvals involved in getting to space. It also identifies areas requiring further effort to fill in policy gaps and "gray areas" in the overall policy picture.

Policy overview

International Treaties and U.S. National Policy

The Outer Space Treaty of 1967[1,2] forms the basis of international space law. It stipulates that states "shall be responsible for national space activities whether carried out by governmental or non-governmental agencies." 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. It further states that 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 domestically owned objects in space, regardless of where the launches took place. Liability for damage falls jointly on the country "from whose territory or facility a space object is launched" and the country that procured the launch; however, 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 negligence or malice.

Within the United States, the 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 document also references "the critical interdependence of space and information systems," which will flow 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 by NASA, and commercial oversight by the Secretary of Transportation; thus, commercial launches are licensed by the Federal Aviation Administration (FAA).

Responsibilities of the Launch Provider vs. the Satellite Owner

The National Space Transportation Policy, true to its name, focuses on space launches, rather than space operations. Similarly, most lower-level policy demarcates the responsibilities of the launch provider and 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. It cannot be, because once launched, these satellites are not necessarily under the authority or direction of the launching agency. Instead, compliance must be enforced through the parent agency of the satellite owner/operator. Thus, a NASA satellite launched on a DoD rocket must comply with NASA policy, not DoD policy. Similarly, a DoD satellite on a commercial launch vehicle must still comply with DoD policy, not commercial policy. Figure 1 illustrates the general responsibilities of mission partners on a launch, and Figure 2 examines how these policy responsibilities break down for a sample multiple-payload mission.

It is important at the beginning of a mission to clarify this demarcation and the proper policy compliance responsibilities for all partners. This approach does not preclude the launching agency from imposing its own more stringent requirements, or even its own parent agency's policies, on the satellites it launches. The launching agency can also "refuse service" to a satellite that does not meet certain requirements, even if those stipulations are not required by policy.

What Constitutes Ownership?

Determining the parent agency of a satellite is critical to understanding the applicable space policy. The flowchart in Figure 3, developed in partnership with the DoD Space Test Program and Air Force Research Laboratory, illustrates a method for determining satellite ownership. The key consideration is, "who will have control authority over the satellite (or payload) once it launches?" For example, 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,

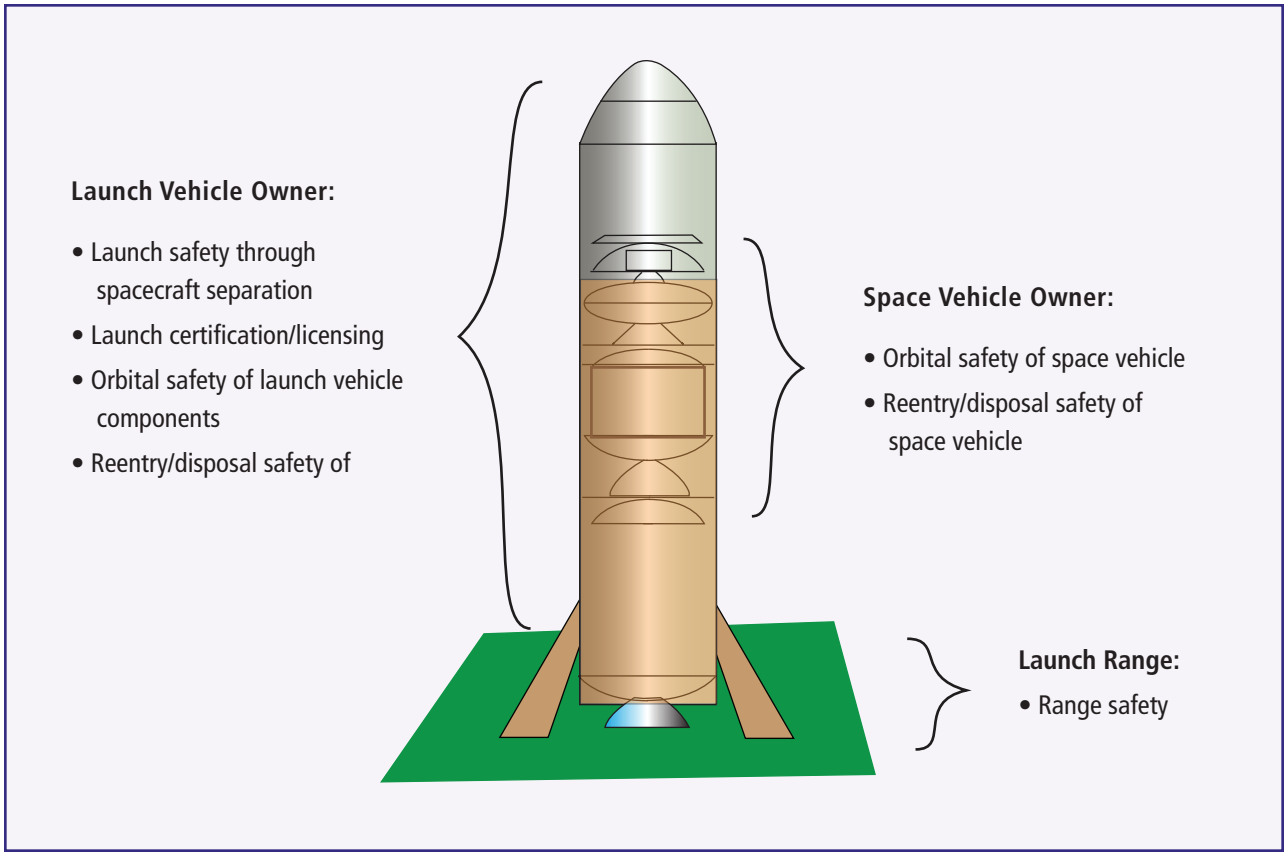


Figure 1: Policy compliance and safety requirements for launch and satellite operations.

with the additional stipulation that NASA contracts and NASA grant recipients are also considered NASA satellites.

Some satellites, however, still fall into gray areas. For example, the Space Test Program frequently arranges for the launch of university satellites sponsored by the DoD Space Experiments Review Board (SERB). Some of these programs also receive small grants from the DoD through educational outreach programs. Although sponsored by the DoD, ownership and control of the satellite remain with the universities. Such payloads follow a commercial path regarding policy regulations, not a DoD path. Discussion continues on this point, however, and further clarity is needed. Also needed are discussions about other "special cases," such as civil government satellites that are not sponsored by the DoD or NASA, and DoD satellites that are not national security space missions.

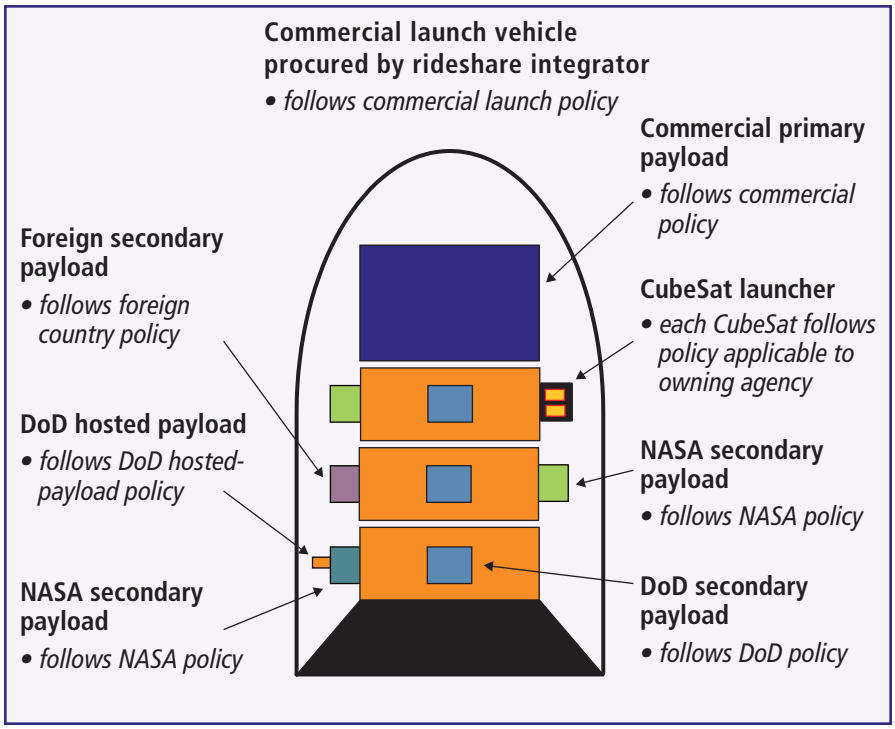


Figure 2: Rideshare policy compliance for individual payloads.

Once the owning organization is identified, the appropriate policies can also be identified. The DoD, NASA, FAA, and Federal Communications Commission (FCC) all have broad policy directives that flow down from the National Space Policy. These include requirements regarding orbital debris mitigation, frequency allocation, information assurance, imaging, and rendezvous and proximity operations.

Orbital Debris

Summary of Applicable Policy

The National Space Policy calls for protection of the space environment from orbital debris. Specifically, one of the Intersector Guidelines directs compliance with U.S. Orbital Debris Mitigation Standard Practices (ODMSP) and requires "the head of the sponsoring department or agency" for space missions to approve exceptions. The ODMSP itself has four sections governing debris generation, accidental explosion, risk of collision with other objects, and disposal of space objects at the end of mission life. Tether systems receive special considerations.

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 Earth, and the requirements that limit the potential for in-space collision, debris generation, and accidental explosion. Other than the 25-year disposal number and the 1 in 10,000 "expectation of casualty" number, the guidance does not contain specific numeric thresholds.

NASA Policy. NASA documents orbital debris mitigation requirements in NASA Procedural Requirements for Limiting Orbital Debris[5] and NASA Process for Limiting Orbital Debris.[6] The latter document imposes specific numeric limits on the probability of in-space collision (1 in 1000 over the lifetime of the mission) and accidental explosion (also 1 in 1000). The document lists other detailed requirements for compliance with the ODMSP. It also requires documentation of compliance in an Orbital Debris Assessment Report and an End of Mission Plan, which must be approved through NASA channels; exceptions flow up through the NASA Office of Safety and Mission Assurance. The National

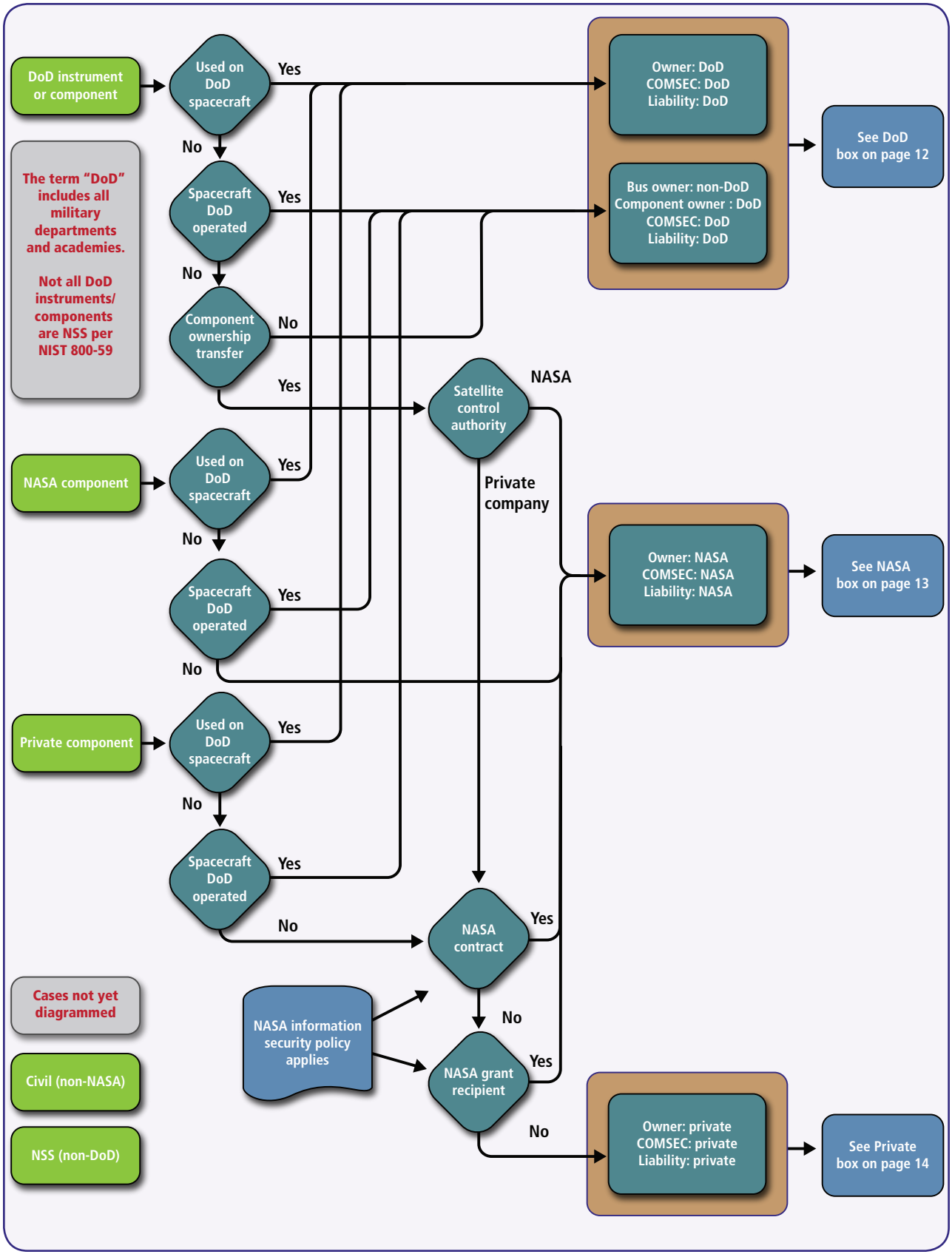


Figure 3: Flowchart for determining space-vehicle ownership. This flowchart attempts to provide a logical walkthrough of policy affecting a particular mission, component, or spacecraft in the areas of positive control, proximity operations, imaging, laser use, and frequency allocation. It is meant to identify applicable policy documents and provide an initial assessment of high-level implementation requirements.

Oceanic and Atmospheric Administration (NOAA) follows NASA's debris mitigation requirements.[7]

DoD Policy. DoD Directive 3100.10, Space Policy,[8] states that the "DoD will promote the responsible, peaceful, and safe use of space, including following the U.S. Government Orbital Debris Mitigation Standard Practices." DoD Instruction 3100.12, Space Support,[9] requires that DoD missions comply with debris mitigation practices that echo the ODMSP. These two directives are implemented in several Air Force Instructions,[10] including 91-217, Space Safety and Mishap Prevention Program,[11] which is similar to the NASA Process for Limiting Orbital Debris. The Air Force documents compliance in a Space Debris Assessment Report for launch vehicles and a combined Space Debris Assessment Report/End of Life Plan for space vehicles, but the format of these documents is essentially the same as the NASA Orbital Debris Assessment Report and End of Mission Plan. Other DoD services have implemented the requirements in DoD Directive 3100.10 in different ways; the National Reconnaissance Office has an Office of Debris Mitigation, while the Army and the Navy have relatively informal coordination processes.

FCC Policy. Private satellites, defined as any satellite not owned or operated by NASA, NOAA, or the DoD, are not bound by NASA and DoD policies but must still comply with orbital debris mitigation guidelines. Compliance is enforced by the FCC through its licensing of uplink and downlink frequencies. Title 47 of the Code of Federal Regulations (47 CFR)[12] 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.[13,14,15]

FAA Policy. The FAA licenses launch and reentry operations for nongovernment launches from U.S. soil or conducted by U.S. companies or citizens. Contrary to popular belief, it does not oversee or regulate satellites 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 casualty on the ground. The FAA, however, does not regulate the disposal of orbiting upper stages.[16]

Orbital Debris: Ambiguity, Open Questions, and Recommendations

The ODMSP represents 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. Another white paper, "US Space Debris Mitigation Regulatory Structure" (M. Sorge, Sept. 2017), discusses the related impacts of the burgeoning commercial space market on U.S. space debris policy. The lack of specific requirements for orbiting upper stages for non-DoD or NASA launches is a gap that policymakers must ultimately address. Also, it is important to note that although the orbital debris compliance requirement is 25 years after mission completion, all satellite owners should strive to dispose of the vehicle as soon as the mission is concluded. 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 in an area where clarity is badly needed.[30]

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 submission of an Orbital Debris Assessment Report and End of Mission Planning in accordance with the NASA Process for Limiting Orbital Debris. The process is similar for Air Force missions, which complete a Space Debris Assessment Report/End of Life Plan in accordance with Air Force Instruction 91-217. Missions without defined processes or formats for

debris compliance can use the NASA Orbital Debris Assessment Report as the template for demonstrating compliance with higher policy, as seems to be the practice for private satellites when requesting licenses from the FCC. Launch vehicles must follow the FAA process through the "end of launch," defined as the last exercise of control over the vehicle. Exceptions to ODMSP guidelines require approval at high levels—the head of the sponsoring department or agency. Such waivers are increasingly difficult to obtain.

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.[17]

Through 47 CFR, the FCC licenses frequency use for nonfederal 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.[18]

The International Telecommunication Union (ITU) is the United Nations group responsible for telecommunications; it does not have authority to enforce policy, but member nations honor its treaty status. It has its own rules and regulations codified in Radio Regulations.[19]

Policy Compliance Process

The NTIA is located within the Department of Commerce and is 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. A subcommittee coordinates and assigns radio frequencies. NASA submissions are reviewed first by the individual NASA center and then by the NASA spectrum management office, which submits the paperwork to the NTIA. DoD missions submit through service-level spectrum management offices, which then submit to the NTIA.

Spectrum Usage: Ambiguity, Open Questions, and Recommendations

Amateur frequencies are strictly protected from use by experimental or federal programs. This has led to some confusion in the community. Until recently, experimental or federally-connected programs regularly used amateur bands. The missions—especially those run by service academies—are now having to determine whether to go through the FCC for an experimental frequency or through the NTIA. For example, satellites built and sponsored by the United States Naval Academy have in the past used amateur frequencies to communicate with an amateur ground station at the Academy. As a federal agency, however, it now appears they should file through the NTIA, and will no longer be allowed to file through the FCC to use amateur frequencies. As of the writing of this paper, the matter has not been resolved, and the resolution has been hampered, in part, by the lack of clear communication between the FCC and the NTIA.

Additionally, there is often confusion for programs that fall into "gray areas." For example, a satellite owned and operated by a university 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.

There are four filing stages for federal programs: conceptual, experimental, developmental, and operational; each is explained in detail in section 10.4.1 of the NTIA manual.17 Most small satellites performing science and technology or research and development missions will obtain a Stage 2 Experimental license. Operational

satellites will obtain a Stage 4 Operational license. Unlike the FCC, the NTIA imposes no requirement to conduct debris or lifetime analysis when applying for frequency authorization.

The FCC is an independent agency (overseen by Congress) that regulates interstate and international communications by radio, television, wire, satellite, and cable. The application and filing process is outlined 47 CFR 25.12 Most small satellites will apply for an amateur or experimental frequency. Amateur frequencies are for communications only, and the operator cannot have a financial interest on behalf of an employer. Experimental frequencies are for conducting experiments.

To use amateur frequencies, a satellite does not need a license, but a licensed amateur operator must submit a prelaunch notification. The operator must also coordinate with the International Amateur Radio Union and include that information with the package to the FCC.

Missions filing with the FCC must demonstrate compliance with ODMSP guidelines. Missions must show that they adhere to debris generation guidelines, will deorbit within 25 years of end of life or move to a disposal orbit, and 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 be approved to broadcast.

When frequency usage is approved, the FCC and NTIA submit their frequency assignments to an FCC liaison, who submits them to the ITU, which maintains the international register. Getting a license or approval to use a frequency through either agency takes months to years, so missions need to start working on the application and submission as early as possible.

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 (CNSS), the National Institute of Standards and Technology (NIST), 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.[20] This instruction implements CNSS Policy No. 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions.[21] To determine if an information system is considered National Security Space, there is NIST Special Publication 800-59, Guideline for Identifying an Information System as a National Security System.[22]

Two DoD Instructions govern cybersecurity compliance for all DoD information systems (not just space systems). They are DoD Instruction 8500.01, Cybersecurity,[23] and the Risk Management Framework for DoD Information Technology.[24] These documents align the DoD with the rest of the federal government by adopting common CNSS and NIST controls, particularly NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.[25] This promotes interoperability, information sharing, and reciprocity, enabling organizations to accept approvals by other organizations for interconnection or reuse of information technology without retesting. The old DoD Information Assurance Certification and Accreditation Process is transitioning to the new Risk Management Framework.

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., encryption). The second concerns certification and accreditation of the spacecraft as an information system (i.e., Authority to Operate).

Encryption. For spacecraft owned or controlled by DoD, 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 National Security Agency (NSA) early in the design phase of every spacecraft program.

For non-DoD federal spacecraft, encryption is not strictly required; however, NIST Special Publication 800-53 does apply, and the criticality and sensitivity of information transmitted may lead to selection of security controls that include encryption. Organizational policies may also apply; for example, NASA Procedural Requirements 2810.1A, Security of Information

Information Assurance: Ambiguity, Open Questions, and Recommendations

The first ambiguity has to do with whether a spacecraft should be considered "DoD" and therefore subject to DoD cybersecurity policy. Differing interpretations abound, with the most stringent classifying any spacecraft receiving DoD sponsorship or funding of any nature as DoD and subject to all DoD policy requirements. This interpretation would have far-reaching implications and is not considered tenable. Satellites should be classified unambiguously based on who owns and operates them. Cybersecurity policy compliance could then be based on the requirements of the owner/operator organization.

A second ambiguity has to do with whether a satellite system falls under the heading of national security space. Not all DoD spacecraft are necessarily national security space systems. NIST Special Publication 800-59 has a checklist with six questions to determine whether an information system is part of a national security space system. Based on this checklist, many DoD scientific spacecraft developed and operated by military laboratories and academic institutions are not national security space systems. As such, CNSS Special Publication 12 is not applicable. However, DoD Instruction 8581.01 (which implements CNSS Special Publication 12) does not provide any provisions for DoD spacecraft that are not considered national security space assets, which drives costly compliance requirements on these programs out of proportion to overall program cost and risk. DoD Instruction 8581.01 should be revised to either explicitly exclude spacecraft that are not for national security or to provide streamlined compliance procedures for them.

DoD 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 upfront.

Finally, there is no policy requiring the protection of non-DoD spacecraft command and control (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 other spacecraft. This is a significant policy gap that will become more pronounced with the increasing capabilities of small satellites and CubeSats. Policy requiring uplink security on all spacecraft with significant maneuver capability would help allay concerns. 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 United States is providing the launch services.

Technology,[26] defines information technology security requirements for NASA.

For commercial or private spacecraft, encryption is not typically required; however, if the DoD is using a commercial, non-DoD federal, or foreign space system, Instruction 8581.01 imposes requirements pertaining to encryption. Depending on the criticality and sensitivity of the information being transmitted, uplink and downlink cryptography may be required ranging from NSA-approved methods to commercial best practices. To obtain a NOAA commercial remote sensing license, rigorous safeguards must be included to ensure the integrity of system operations and the security of its data. Early coordination with NSA is recommended.

Certification and Accreditation. DoD Instruction 8581.01 requires that all DoD-owned systems undergo cybersecurity accreditation in accordance with the Risk Management Framework. A full discussion of this

framework is beyond the scope of this paper; however, two points are worth mentioning. Each DoD spacecraft program should identify a cybersecurity Authorizing Official early on; this official will ultimately issue the Authority to Operate for the spacecraft.

Non-DoD federal spacecraft must follow their own internal policies regarding accreditation. Recent experience with NASA indicate that formal certification and accreditation of the spacecraft is typically not required. For example, for the Green Propellant Infusion Mission, NASA was required to issue an Authority to Operate, but only because the spacecraft will be operated on an accredited DoD ground system.

Commercial and private spacecraft have no requirements to undertake a formal cybersecurity accreditation. When the DoD is using non-DoD systems, Instruction 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 noncompliance.

Imaging

Summary of Applicable Policy

Regulations governing remote sensing from a space platform fall into two distinct categories in the United States: Earth imaging and non-Earth imaging. Two types of satellites are considered: commercial (civilian) and government. Satellites owned by DoD academic institutions are considered a subtype of government-owned satellites and fall into their own unique policy bucket.

Satellites owned and operated by commercial entities and civilian academic institutions are governed by the National Commercial and Space Programs Act.[27] This law governs Earth-imaging and assigns licensing authority to NOAA, which will also ensure all imagers comply with DoD and intelligence community requirements for non-Earth imaging.

Government agencies currently have no requirement to obtain licensing for Earth imaging. 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.[28] This interim guidance, issued in 2015, requires programs to submit test plans, data-protection plans, and technical specifications of their system and payloads to the Principal DoD Space Advisor Staff, through the Secretary of the Air Force Space Programs office. Any concerns are automatically referred to the Defense Remote Sensing Working Group.

NASA has not published any guidance or documentation with respect to imaging approval. All imaging devices aboard NASA satellites and missions are handled internally.

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, nonbinding meetings between the applicant and NOAA to help inform the process and prevent rework. When an

Imaging: Ambiguity, Open Questions, and Recommendations

It is unclear what, exactly, constitutes "imaging" for the purposes of policy compliance. For example, most satellites have star trackers, which help identify and control spacecraft attitude. Although imaging is not their primary function, these star trackers do contain cameras that could image the Earth or other objects in space, either intentionally or inadvertently. Historically, star trackers have not been subject to imaging approval, but anecdotal evidence suggests that may be changing. Overly regulating such devices will make it difficult for satellites—especially small satellites—to complete their designs, and greater clarity is needed.

The DoD and the federal government are developing clearer policy guidance for military academic institutions and satellites that receive funding from DoD but are not owned by DoD. Until this definition is provided in final guidance, organizations will potentially receive conflicting answers from policy staff.

organization is prepared to begin the application process, 15 CFR 960[29] establishes the rules and procedures to be followed, and NOAA provides support to ensure all the required documentation is provided. All license determinations must be made within 120 days of receipt of a completed application unless written guidance is provided on existing issues. All licenses are valid for the operational lifetime of the system unless voided through action of the owner or operator.

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 spacecraft into the vicinity of another. Current policy in this area involves a patchwork of guidance documents from across the space community. As the capability of small satellites increases, so does the potential for proximity operations. Spacecraft designers must balance the need to perform mission objectives with the need to maintain flight safety—because the debris from a collision affects the entire space environment, not just the two satellites involved. Safety concerns extend to formation-flying satellites, which are designed to maintain a constant distance relative to each other. NASA has no policy guidance concerning proximity operations. A DoD policy covers the review of proximity operations, but this may not be 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 must comply with DoD processes. Civil and commercial entities are not required to comply with any process unique to proximity operations, although missions will naturally need to comply with all frequency and imaging requirements discussed above.

Policy Flowchart: A Sample Walkthrough

Figures 4 through 6 summarize the policy pathways described in this paper.

As an example, if the Air Force Research Laboratory builds a satellite 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 NSA-approved encryption. Such a satellite would apply to the NTIA for frequency assignment and must adhere to DoD regulations governing proximity operations.

As another example, assume a private company builds a satellite capable of imaging and stationkeeping, and brings it to the DoD Space Experiments Review Board for consideration. Even with Review Board sponsorship, the satellite is still considered a commercial/private satellite and will follow public policy for privately-owned satellites. It will apply for a frequency license through the FCC and apply for imaging approval

Rendezvous and Proximity Operations: Ambiguity, Open Questions, and Recommendations

The growth in capability of small satellites has brought about a surge in missions involving formation flying, rendezvous, proximity operations, and docking. Due to the technical challenges and flight safety concerns inherent in such missions, clarification on processes for civil and commercial entities would be beneficial. The policy could distinguish between formation flying and proximity operations based on the distance between the vehicles and define policy guidance for each class. Designers of formation and proximity missions would do well to comply with NIST 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) is cybersecurity requirements for vehicles with propulsion, regardless of their intention to conduct proximity operations. Key to this guidance should be directives based on how much vector change a vehicle can achieve. 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 simple attitude-control propulsion systems.

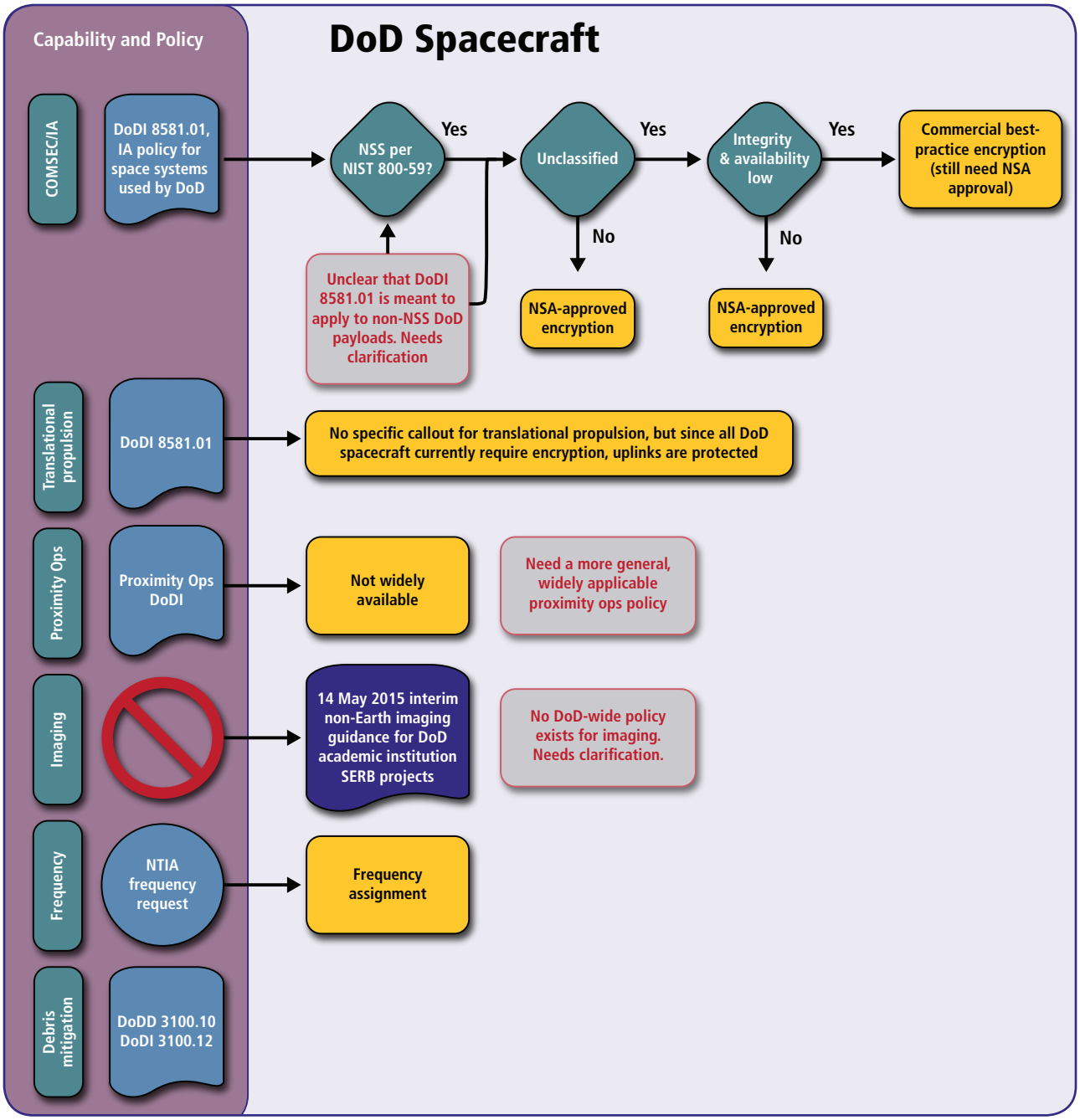
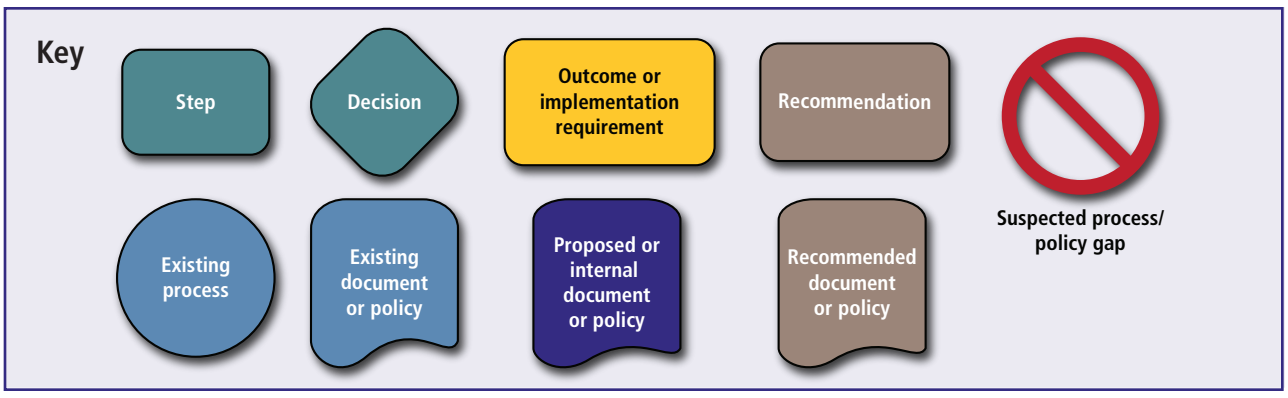


Figure 4: Policy roadmap flowchart for DoD spacecraft.



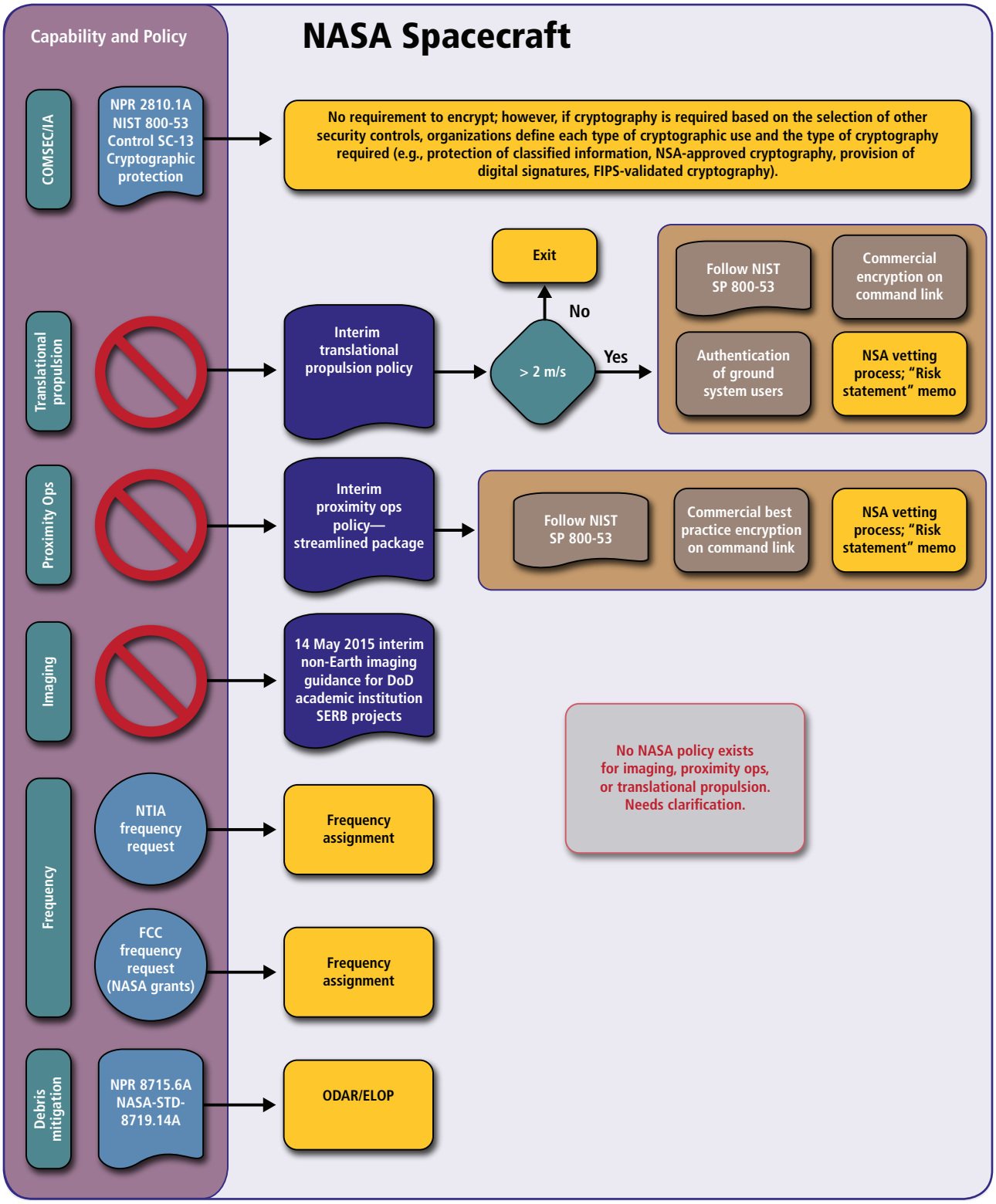


Figure 5: Policy roadmap flowchart for NASA spacecraft.

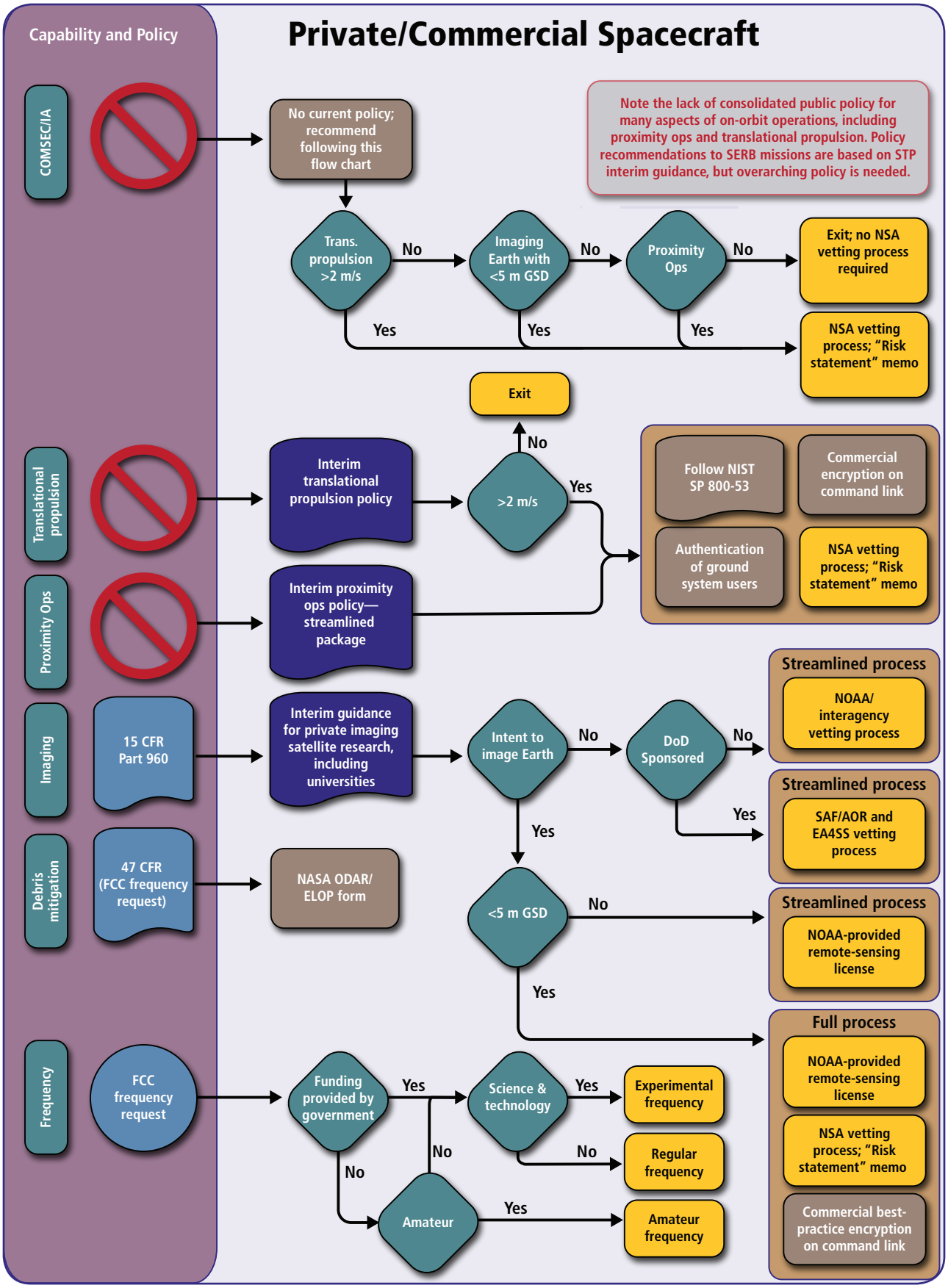


Figure 6: Policy roadmap flowchart for private/commercial spacecraft.

through NOAA. As part of its FCC filing, it will demonstrate compliance with the ODMSP. The company is not required to encrypt the satellite uplink or downlink, nor is it required to get approval for proximity operations. These are policy gaps that must be filled.

An enterprise architecture approach across oversight and regulatory silos can transform and improve the compliance experience. Figure 7 is a conceptual representation of a centralized government gateway or one-stop-shop, which could transform the current labyrinthine process. A centralized government gateway could help satellite mission owners determine into which policy and oversight "bucket" they fall (government, civil, or private), depending on who controls the mission and what funding they receive. The gateway could then help facilitate policy approvals by routing paper-work to the correct regulatory agencies. This would help avoid policy loopholes, and ensure "gray area" missions are properly dispositioned.

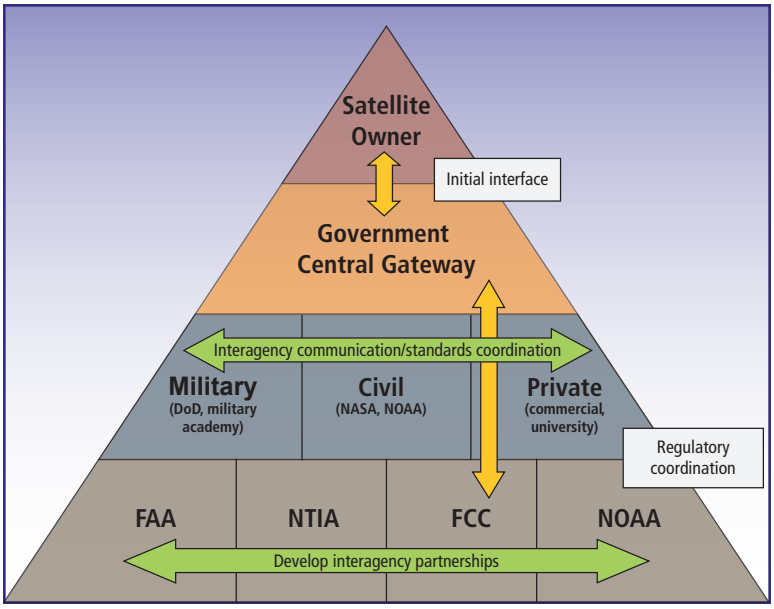


Figure 7: Conceptual government policy gateway. Regulatory coordination appears unified and transparent to the end customer.

From the top tier down: Owners vet internal policy and strategy. Owners coordinate with a centralized government gateway, which confirms whether military, civil, or private policy should be applied, determines what regulatory approvals are required, and assists in coordinating approvals. Owning agency enforces appropriate policy; agencies coordinate to ensure similar standards where possible.

Conclusion

The policy picture for today's rapidly-evolving space enterprise is complex and confusing, particularly for nontraditional entrants and missions that occupy policy "gray areas." This paper has attempted to clarify the applicability of existing policy and outline a process to ensure compliance. In some cases, policy is absent or unclear. It is, however, important to remember that the policy roadmap is always "under construction," and future changes are certain.

There is increased demand across the globe for governments to find ways to improve the efficiency and effectiveness of service delivery. The space community regulatory environment should be no exception to this trend; however, transformation will require time and broad participation from stakeholders, and interagency regulatory relationships will require legislative attention. The proposed American Space Commerce Free Enterprise Act of 2017, for example, includes provisions to designate a single authority for commercial space activities (in this case the Secretary of Commerce).

The tempo of space launches is expected to increase, with several new large constellations being planned. As the space enterprise evolves, U.S. policy must be agile enough to evolve with it, to ensure both access to space and safety in space for all.

Acknowledgements

The authors would like to acknowledge Ken Reese and David Butzin from the DoD Space Test Program and Austin Potter and David Voss of the Air Force Research Laboratory 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" (Oct. 10, 1967, United Nations, New York).

[2] "The Outer Space Treaty: Assessing Its Relevance at the 50-Year Mark" (July 2017, 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" (June 28, 2010).

[4] "National Space Transportation Policy" (Nov. 21, 2013).

[5] "NASA Procedural Requirements for Limiting Orbital Debris" (NPR 8715.6A) (May 14, 2009).

[6] "NASA Process for Limiting Orbital Debris (NASA STD 8719.14A)" (May 25, 2012).

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

[8] "DoD Directive 3100.10: Space Policy" (Oct. 18, 2012).

[9] "DoD Instruction 3100.12: Space Support" (Sept. 14, 2000).

[10] "Air Force Instruction 91-202: The US Air Force Mishap Prevention Program" (June 24, 2015)

[11] "Air Force Instruction 91-217: Space Safety and Mishap Prevention Program" (April 11, 2014)

[12] "Code of Federal Regulations Title 47: Telecommunications" (Apr. 19, 2016)

[13] "Dove 3 Orbital Debris Assessment Report" (Oct. 9, 2012, Cosmogia, San Francisco).

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

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

[16] "Space Debris Mitigation Policy," Crosslink (Fall 2015, The Aerospace Corporation, El Segundo, CA).

[17] "Manual of Regulations and Procedures for Federal Radio Frequency Management" (NTIA, May 2014).

[18] "Guidance on Obtaining Licenses for Small Satellites" (FCC, March 15, 2013); DA-13-445A1_Rcd.pdf.

[19] "Radio Regulations" (2012, World Radiocommunication Conferences, ITU, Geneva).

[20] "DoD Instruction 8581.01: Information Assurance Policy for Space Systems" (June 8, 2010).

[21] "Committee on National Security Space Policy No. 12: National Information Assurance Policy for Space Systems Used to Support National Security Missions" (Nov. 28, 2012, Committee on National Security Systems, Ft Meade, MD).

[22] "NIST Special Publication 800-59: Guideline for Identifying an Information System as a National Security System" (Aug. 2003).

[23] "DoD Instruction 8500.01: Cybersecurity" (Mar. 12, 2014).

[24] "Risk Management Framework for Department of Defense Information Technology" (Mar. 12, 2014).

[25] "NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations" (Apr. 2013)

[26] "NASA Procedural Requirements for Security of Information Technology (NPR 2810.1A)" (May 16, 2006).

[27] "United States Code Title 51: National Commercial and Space Programs" (Dec. 18, 2010).

[28] "Interim Non-Earth Imaging Guidance for DoD Academic Institution SERB Projects" (Nov. 3, 2015).

[29] "Code of Federal Regulations Title 15 Part 960" (Apr. 25, 2006).

[30] M. Sorge, "U.S. Space Debris Mitigation Regulatory Structure," The Aerospace Corporation (Sept. 2017).