

Policy Considerations for Orbital Data Centers

ELLIS SCHERER AND ELIZABETH SANCHEZ | SEPTEMBER 2026

Orbital data centers could complement terrestrial infrastructure by processing selected workloads in space, particularly where data is generated in orbit. Their value will depend on technical performance, life cycle economics, market demand, and a regulatory environment that does not hinder testing and deployment.

KEY TAKEAWAYS

- Orbital data centers are more likely to complement—not replace—terrestrial data centers, with near-term potential concentrated in specialized, space-based workloads.
- Processing data in orbit could reduce downlink demands and improve responsiveness for applications such as Earth observation, remote sensing, and spacecraft autonomy.
- Thermal management, radiation, communications capacity, limited servicing, cybersecurity, and launch costs remain significant technical and economic constraints.
- Policymakers should ensure access to ample spectrum, streamline satellite licensing, clarify cybersecurity requirements, expand and update launch infrastructure, and address orbital sustainability.

CONTENTS

Key Takeaways..... 1

Introduction..... 2

Why Orbital Data Centers Are Gaining Relevance 3

Advantages of Orbital Computing 3

Technical and Economic Challenges for Orbital Data Centers..... 4

Policy Challenges and Recommendations for Orbital Data Centers..... 7

Conclusion 9

Endnotes..... 10

INTRODUCTION

Orbital data centers are specialized satellites that support computing functions by processing data in space.¹ This emerging technology is attracting growing attention amid both rising demand for computing capacity and advances in commercial space capabilities.² As the global space economy continues to grow and more digital services rely on space-based infrastructure, orbital computing may become useful for selected space-based workloads. Government assessments, technical research, and industry feasibility studies are currently examining whether selected computing functions could be performed in orbit for specialized applications, although significant engineering and economic questions remain.³

Today’s orbital data center concepts should not be understood as near-term substitutes for terrestrial cloud infrastructure.⁴ Data centers on Earth benefit from mature supply chains, easier repair and upgrade cycles, and lower operating complexity. Orbital systems, by contrast, must operate in a harsher environment that includes radiation exposure, thermal management challenges, communications constraints, and high deployment and replacement costs.⁵ If orbital compute clears current technical and economic hurdles, then the central policy consideration is whether orbital systems can perform specialized computing functions well enough to justify their operational complexity rather than whether they can replace terrestrial hyperscale data centers.

Orbital computing can reduce bandwidth demands and improve operational responsiveness, particularly where decisions must be made in orbit rather than on the ground.

The strongest near-term opportunity for orbital computing lies in workloads that benefit from processing data where it is generated in space. These include Earth observation, remote sensing, and onboard spacecraft autonomy.⁶ Over a longer time horizon, onboard or distributed computing could also become useful for certain lunar and cislunar missions, particularly where communications architecture or operational requirements favor local processing. In such settings, orbital computing may reduce bandwidth demands and improve operational responsiveness, particularly where decisions must be made in orbit rather than on the ground.⁷

For that reason, orbital data centers are best treated as a complementary layer of digital infrastructure rather than a wholesale replacement for terrestrial systems.⁸ Public policy should focus on ensuring that existing regulatory frameworks allow markets to identify and develop those applications for which orbital computing offers genuine comparative advantages, which could lead to orbital systems becoming a meaningful complement to the broader digital infrastructure ecosystem.

WHY ORBITAL DATA CENTERS ARE GAINING RELEVANCE

The simultaneous increase in demand for compute-intensive services alongside the improvement of commercial space capabilities is generating interest in orbital data centers. The Government Accountability Office's (GAO's) April 2026 "Science & Tech Spotlight" describes space-based data centers as "satellites that would house data processing and storage systems for AI and other computing needs," potentially reducing the land, electricity, and water required by terrestrial facilities.⁹ This framing, in the context of resistance to expanding terrestrial data center infrastructure, helps explain why the concept is now receiving policy attention, even though the underlying technology remains in an early stage.¹⁰

Orbital data centers may eventually complement terrestrial infrastructure in specialized use cases.

Private-sector research has reinforced that interest. Google's Project Suncatcher is an exploratory initiative that examines the feasibility of scaling machine-learning compute in space using solar-powered satellite constellations, special processors, and free-space optical communications links.¹¹ Thales Alenia Space's ASCEND project likewise presents space-based data centers as a feasibility question, indicating that orbital computing has become the subject of structured technical and commercial investigation.¹²

The broader relevance is that orbital computing may become a useful layer of digital infrastructure for specific workloads before it becomes competitive with terrestrial cloud infrastructure.¹³ A space-based architecture that is appropriate for one mission class may still be uneconomical for general-purpose computing, particularly where latency, maintenance, replacement, and scale economies continue to favor Earth-based facilities. Therefore, the current evidence supports measured attention rather than exaggerated expectations.

Orbital data centers may eventually complement terrestrial infrastructure in specialized use cases, but their near-term significance will depend on whether the technical and economic constraints can be managed at acceptable costs. The role for policymakers is to create a regulatory environment that minimizes unnecessary barriers to testing and deploying this new technology. The true value of orbital data centers will be easier to assess once these regulatory barriers are reduced.

ADVANTAGES OF ORBITAL COMPUTING

The most plausible near-term case for orbital computing is mission-specific data processing. When data is generated and processed in orbit, and only a subset is transmitted back to Earth, orbital data centers may reduce the volume of transmitted data and, in some missions, improve operational responsiveness.¹⁴ That logic is especially relevant for Earth observation, remote sensing, spacecraft autonomy, and other space-native tasks.

A related but more contingent possibility is that orbital systems could reduce certain site-specific terrestrial infrastructure pressures in selected applications. GAO notes that space-based data centers could reduce the overall land, electricity, and water needs of data centers on Earth, while Google's Project Suncatcher similarly frames space-based compute as capable of lessening the strain on terrestrial resources.¹⁵

These potential benefits would materialize only in certain system configurations, and they are not evidence that orbital data centers will be cost competitive for general-purpose cloud computing workloads. Whether those advantages matter in practice will depend on the full life cycle economics of launch, servicing, communications, replacement, and orbital operations.¹⁶ Thus, the relevant question is not whether orbital computing is superior in the abstract, but whether it offers a net advantage for certain operations once engineering constraints and life cycle costs are fully accounted for.¹⁷

For policy purposes, the key implication is that orbital data centers should be evaluated use case by use case rather than treated as a single integrated market. If regulatory compliance costs are minimized and equal across use cases, then the actual costs of each are limited to the technology itself, which provides clarity on which use cases genuinely benefit from orbital computing. Minimizing regulatory costs can be achieved through transparent compliance requirements and streamlined licensing procedures, as is discussed in more detail later in this report.

The case for orbital computing will vary by workload and mission; policy should reflect those differences rather than treat the sector as a single market.

TECHNICAL AND ECONOMIC CHALLENGES FOR ORBITAL DATA CENTERS

Orbital data centers face substantial engineering and economic constraints. Available technical studies identify radiation exposure, thermal management, communications capacity, limited servicing, cybersecurity, and system resilience as the recurring challenges in their design and operation.¹⁸

Thermal management is the most significant engineering constraint. Computing equipment generates substantial waste heat that must be removed to maintain acceptable operating temperatures. Terrestrial data centers can manage this heat through air- and liquid-based cooling systems that ultimately transfer waste heat to the surrounding environment.¹⁹ In the vacuum of space, spacecraft cannot reject heat to the surrounding environment via convection and must reject internally generated waste heat through thermal radiation.²⁰ This engineering challenge creates trade-offs involving radiator area, spacecraft design, mass, and power density that can constrain system scale and performance.²¹ Even where an orbital system can obtain substantial solar energy, heat rejection may remain a major design constraint.²²

Radiation is another engineering challenge for orbital data centers. Depending on the orbit, shielding, component selection, and mission duration, exposure to ionizing radiation and energetic particles can increase fault risk, degrade component performance, and shorten hardware lifetimes.²³ Radiation-hardening and other mitigation techniques can improve tolerance

and limit damage. Still, radiation hardening adds costs associated with a satellite's mass, power, performance, hardware resources, and engineering complexity.²⁴

Maintenance and upgrade cycles in orbit differ substantially from those of terrestrial data centers. Terrestrial data centers can be serviced, expanded, and refreshed comparatively easily, but orbital systems face limited opportunities for repair and replacement.²⁵ Because physical servicing in orbit remains difficult, costly, and unavailable for many architectures, hardware failures may be substantially harder to repair than in terrestrial data centers. Furthermore, rapid changes in computing technologies in hyperscale data centers may lead to technological obsolescence if satellite deployment schedules are not aligned with hardware advances.²⁶ This dynamic effectively shortens the usable life cycle of orbital hardware relative to its terrestrial counterpart, which translates directly into higher life cycle costs than for a comparable terrestrial deployment.

Hardware failures in orbit can be substantially more difficult to address than in terrestrial data centers, increasing the importance of redundancy, fault tolerance, and system resilience.

These engineering and economic constraints are compounded by a set of cybersecurity and data governance concerns that have no straightforward terrestrial equivalent. Their attack surface may span spacecraft, communications links, ground infrastructure, and cloud management systems. Command channels and telemetry may be vulnerable to spoofing or unauthorized access; radio-frequency links may be subject to jamming; and supply-chain compromise, malicious firmware, or insider threats may affect both space and ground components.²⁷ Depending on the architecture, mission, data, technology, and jurisdictions involved, operators may also encounter export-control and government-access requirements, as well as privacy and data-governance considerations.²⁸

For example, depending on the architecture and mission, U.S. operators may be subject to Federal Communications Commission (FCC) licensing requirements and, wherever a system operates regulated remote-sensing capabilities, National Oceanic and Atmospheric Administration (NOAA) licensing under 15 C.F.R. Part 960.²⁹ Depending on the technology, data, and other characteristics of the system, export-control restrictions or other sector-specific legal obligations may also apply.³⁰

Because spacecraft are often difficult or impossible to repair once deployed, cybersecurity and resilience should be incorporated throughout system design, development, and operations.

In addition, federal policy and guidance, such as Space Policy Directive-5 and National Institute of Standards and Technology (NIST) cybersecurity guidance, establish cybersecurity principles and recommended practices relevant to commercial space systems.³¹ Collectively, these authorities address different aspects of space operations, communications, remote sensing, export controls, and cybersecurity, but no single generally applicable federal framework governs orbital computing as an integrated space-and-ground network architecture.

Because spacecraft are often difficult or impossible to repair once deployed, cybersecurity and resilience should be incorporated throughout system design, development, and operations. Relevant measures include strong encryption and authentication, resilience planning, and

supply-chain risk management. Existing federal cybersecurity frameworks can provide a starting point for managing risks across the space and ground segments.³²

Together, these operational, security, and governance burdens suggest that early orbital data center applications are more likely to involve specialized, mission-driven workloads than general cloud substitution. That overhead is easier to justify for workloads with distinct requirements than for commodity computing that terrestrial infrastructure already handles well. In-orbit processing may offer commercial value if it reduces downlink burdens, supports spacecraft autonomy, or handles workloads for which timeliness matters more than raw cost per unit of compute.³³ Terrestrial data centers are likely to remain the default platform for broad commercial computing because they benefit from mature infrastructure, established business models, and simpler maintenance and upgrade cycles.³⁴

Figure 1: Comparison of terrestrial and orbital data centers

Dimension	Terrestrial Data Centers	Orbital Data Centers
Location	On the ground in facilities near power, networks, and users	In space (LEO, MEO, GEO); remote from the space environment
Power	Robust, low-cost electricity from terrestrial grids	Architecture dependent; solar power can be abundant, but generation, storage, distribution, and eclipse periods constrain system design
Cooling & Heat Rejection	Mature, cost-effective air or liquid cooling solutions	Waste heat must be rejected radiatively, radiator area, mass, geometry, and power density can limit system design
Maintenance & Upgrades	Routine physical access; hardware can be repaired or updated regularly	Difficult or impossible to access; hardware must be highly reliable
Latency to Users	Low latency for local/regional users on terrestrial networks	Architecture dependent; can reduce latency for space-native processing but increase latency for certain terrestrial users
Bandwidth & Data Links	High-bandwidth fiber networks with redundancy	Spectrum and link capacity often limited; variable conditions and line-of-sight constraints
Environment & Reliability	Controlled environment with proven operational history	Exposure to radiation and thermal cycling; reliability requirements depend on orbit, mission duration, and system design
Scale & Cost Today	Large scale at lower cost per compute dollar	Early stage; life cycle economic remain uncertain and deployment costs are significant
Best Suited For	General-purpose workloads, cloud services, AI/ML training, and storage	Space-native data processing, ISR, autonomy, space science, remote sensing, and edge processing
<i>Orbital data centers are not a replacement for terrestrial data centers, rather, they are potentially complementary for specific workloads that leverage in-space processing advantages.</i>		

POLICY CHALLENGES AND RECOMMENDATIONS FOR ORBITAL DATA CENTERS

Policymakers should reduce unnecessary regulatory barriers to experimentation to effectively measure the benefits of orbital data centers. This reduction includes removing constraints on spectrum access, streamlining inefficient licensing, addressing launch-capacity constraints, and accounting for externalities such as orbital debris and cybersecurity risk.

These reforms are needed because spectrum is a necessary resource to enable the compute functions that may make orbital data centers useful. Slow licensing and launch capacity constraints prevent iterative testing capabilities by blocking orbital data centers from launching frequently enough to extract critical performance data. Insurmountable cyber vulnerabilities and an overly congested orbital environment risk making orbital data centers a nonstarter before they have been fully tested.

Orbital data centers will need reliable spectrum access for space-to-ground, ground-to-space, and space-to-space communications. The FCC's *Spectrum Abundance for Weird Space Stuff* proceeding is considering measures to clarify access to existing spectrum allocations and make additional spectrum available for telemetry, tracking, and command, and other emerging space operations.³⁵ More generally, uncertainty around spectrum rights and coordination procedures can increase transaction costs and deter investment. Clearer rules and more efficient licensing could reduce regulatory uncertainty and unnecessary administrative barriers. The FCC has adopted reforms to modernize its satellite and earth station licensing framework, and is investigating ways to create more spectrum for launch, reentry, and in-orbit activities.³⁶ As new satellite technology combines communications, computing, storage, and other functions, certain orbital data center architectures may nevertheless raise questions about how existing licensing and spectrum requirements will apply to emerging hybrid systems. Regulatory agencies should proactively determine how emerging technology such as orbital data centers will fit within current compliance regimes or begin developing new regulations that account for next-generation systems. Doing so will prevent regulatory drag on orbital data center testing and deployment.

Orbital data centers will need reliable spectrum access for space-to-ground, ground-to-space, and space-to-space communications.

The FCC, through its existing administrative authority, can ensure that regulation does not lag behind innovation—and it should proactively do so. Additionally, Congress could complement those efforts through legislation like the SAT Streamlining Act, which establishes additional statutory requirements intended to increase the predictability and timeliness of satellite licensing.³⁷

Licensing reform alone will not be sufficient if launch capacity cannot support deployment, as some proposed large-scale architectures could depend on heavy-lift launch capabilities and a high launch cadence to deploy in orbit. Congress should evaluate spaceport modernization and launch-infrastructure investment in light of demonstrated capacity needs, broader government and commercial launch demand, and public benefits.³⁸ Where infrastructure constraints are demonstrated, policymakers should prioritize investments and regulatory reforms that expand

launch capacity while accounting for budgetary trade-offs and preserving competition among commercial launch providers.

Orbital computing may test how existing regulatory categories apply as space systems increasingly combine communications, computing, storage, and other functions.

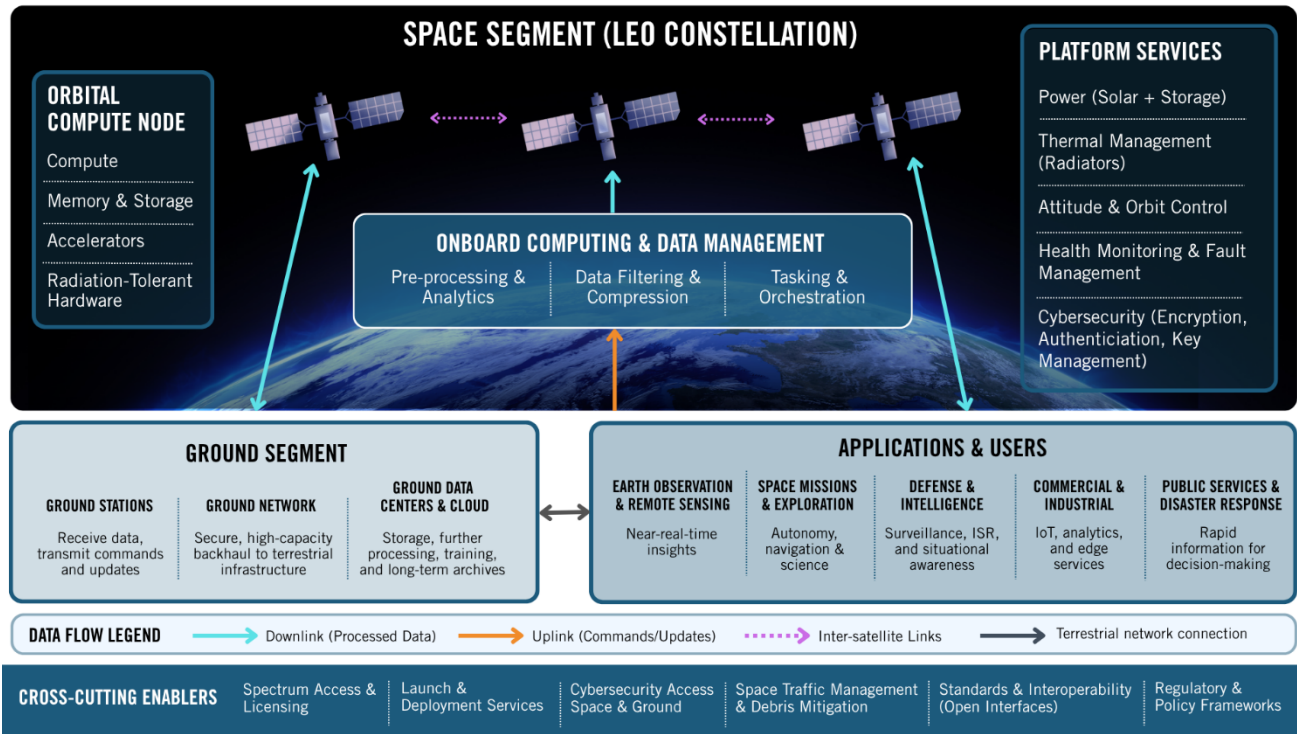
More launches also mean more satellites in orbit, raising separate sustainability concerns. As the space ecosystem continues to grow, orbital data centers would place additional satellites into increasingly congested orbital regimes, heightening the importance of debris mitigation, tracking, conjunction assessment, and space traffic coordination. Policies like the ORBITS Act would address active debris remediation and related sustainability practices. At the agency level, NOAA's Office of Space Commerce is deploying the Traffic Coordination System for Space to provide basic space situational awareness and spaceflight-safety services to civil and private operators.³⁹ Measures that improve debris mitigation, space traffic coordination, and conjunction awareness can improve the safety and predictability of the orbital environment for continued space operations.⁴⁰

Finally, regulatory agencies should clarify how existing cybersecurity expectations apply to orbital compute architectures, including software assurance, encryption and authentication, identity management, supply-chain risk management, and incident response across the space and ground segments.⁴¹ For government-facing systems, federal acquisition processes can provide a mechanism for incorporating cybersecurity and software supply chain risk management considerations into procurement decisions. For commercial systems, voluntary guidance and risk-based frameworks may help operators manage cybersecurity risks without prematurely locking in rigid technical mandates.⁴² Cross-border coordination also matters because data routing, launch services, component sourcing, and ground-station access often span jurisdictions with different security, export-control, and data-governance rules.

Policy should enable experimentation while allowing technical performance, economics, and market demand to determine where orbital computing creates genuine value.

These recommendations reflect a common principle: minimize unnecessary regulatory friction while preserving the safeguards necessary for safe experimentation. The goal is not to subsidize orbital data centers into existence or to presume that they will scale broadly; it is to ensure that the regulatory frameworks avoid unnecessary barriers to testing while preserving legitimate safeguards for spectrum, safety, cybersecurity, national security, and orbital sustainability.

Figure 2: Rendering of a potential orbital data center system



CONCLUSION

As orbital data center technologies evolve, policymakers should focus on reducing unnecessary regulatory uncertainty, improving the predictability of spectrum access and licensing, clarifying cybersecurity expectations, and improving the safety and predictability of an increasingly congested orbital environment. These measures can lower barriers to experimentation while preserving appropriate safeguards for competition, national security, orbital sustainability, and the reliable operation of critical communications infrastructure. Whether orbital data centers ultimately become a meaningful component of digital infrastructure should depend on demonstrated technical performance, life cycle economics, customer demand, and operational reliability—not on regulatory inertia or policy-driven preferences.

Acknowledgements

Thank you to our colleague Mina Kim for her thoughtful and in-depth contributions to this report. Her expertise was critical in establishing a clear understanding of the relevant technical, engineering, and economic challenges shaping the policy discussion on orbital data centers.

About the Authors

Ellis Scherer is a policy analyst at ITIF covering broadband, spectrum, and space policy. He previously interned with the National Telecommunications and Information Administration (NTIA) and worked as a cybersecurity consultant. He holds a master's degree in terrorism and homeland security policy from American University and a bachelor's degree in politics and history from the University of California, Santa Cruz.

Elizabeth L. Sanchez is a policy fellow at ITIF covering broadband, spectrum, and space policy. She previously worked in private practice, multinational corporations, and international organizations. She is a Mexican-qualified attorney and holds an LL.M. in Technology Law & Policy from Georgetown University Law Center.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. Karen Howard, "Science & Tech Spotlight: Data Centers in Space" (U.S. Government Accountability Office, April 2026), <https://www.gao.gov/assets/gao-26-109012.pdf>.
2. Travis Beals, "Exploring a space-based scalable AI infrastructure system design" (Google Research, November 4, 2025), <https://research.google/blog/exploring-a-space-based-scalable-ai-infrastructure-system-design/>.
3. Thales Alenia Space, "Thales Alenia Space reveals results of ASCEND feasibility study on space data centers," news release, June 27, 2024, <https://www.thalesaleniaspace.com/en/press-releases/thales-alenia-space-reveals-results-ascend-feasibility-study-space-data-centers-0>.
4. Howard, "Science & Tech Spotlight."
5. Nathan Bleier and Rakesh Kumar, "Space Data Centers," *Computer* (June 2026), <https://www.computer.org/csdl/magazine/co/2026/06/11540007/2gT4OZL8NvG>; Nathan Bleier et al., "Space Microdatacenters" (paper presented at the 56th Annual IEEE/ACM International Symposium on Microarchitecture, Toronto, Ontario, Canada, October 28–November 1, 2023), <https://passat.crhc.illinois.edu/micro23.pdf>; Nathan Bleier et al., "Architecting Space Microdatacenters: A System-level Approach" (paper presented at the 2025 IEEE International Symposium on High Performance Computer Architecture, Las Vegas, Nevada, March 1–5, 2025), <https://ieeexplore.ieee.org/document/10946786>.
6. Bleier and Kumar, "Space Data Centers."

7. National Aeronautics and Space Administration, “Onboard Processing for LunaNet Data Services” (2025); Bradley Denby and Brandon Lucia, “Orbital Edge Computing: Nanosatellite Constellations as a New Class of Computer System,” *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '20)* (2020).
8. Davide D'Ambrosio et al., *Energy and AI* (International Energy Agency, April 2025), <https://iea.blob.core.windows.net/assets/de9dea13-b07d-42c5-a398-d1b3ae17d866/EnergyandAI.pdf>; Howard, “Science & Tech Spotlight.”
9. Howard, “Science & Tech Spotlight.”
10. Robin Gaster, “The United States Needs Data Centers, and Data Centers Need Energy, but That Is Not Necessarily a Problem” (ITIF, November 2025), <https://itif.org/publications/2025/11/24/united-states-needs-data-centers-data-centers-need-energy-but-that-is-not-necessarily-a-problem/>.
11. Beals, “Exploring a space-based scalable AI infrastructure system design.”
12. Thales Alenia Space, “ASCEND feasibility study on space data centers.”
13. Howard, “Science & Tech Spotlight.”
14. Denby and Lucia, “Orbital Edge Computing;” Bleier and Kumar, “Space Data Centers.”
15. Howard, “Science & Tech Spotlight;” Beals, “Exploring a space-based scalable AI infrastructure system design.”
16. Luca Bennici and Philip Johnston, “The case for data centers in space,” McKinsey & Company, May 8, 2026, <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-case-for-data-centers-in-space#/>; Jesse Noffsinger et al., “The Cost of Compute: A \$7 Trillion Race to Scale Data Centers,” McKinsey & Company, April 28, 2025, <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-cost-of-compute-a-7-trillion-dollar-race-to-scale-data-centers>.
17. Bleier et al., “Architecting Space Microdatacenters.”
18. Ibid.
19. Ashley J. Lawson et al., “Data Centers and Their Energy Consumption: Frequently Asked Questions” (Congressional Research Service, May 12, 2026), https://www.congress.gov/crs_external_products/R/PDF/R48646/R48646.8.pdf.
20. Andrew Cavalier, “Why Orbital Data Centers are Harder Than Silicon Valley Thinks,” *IEEE Spectrum*, June 11, 2026, <https://spectrum.ieee.org/orbital-data-centers-heat>.
21. Ibid.
22. Ibid.
23. Beals, “Exploring a space-based scalable AI infrastructure system design.”
24. Bleier et al., “Architecting Space Microdatacenters.”
25. Ibid.
26. Beals, “Exploring a space-based scalable AI infrastructure system design.”
27. President Donald J. Trump, “Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems” (September 4, 2020), <https://www.transportation.gov/sites/dot.gov/files/2023-11/Memorandum%20on%20Space%20Policy%20Directive-5%E2%80%9494Cybersecurity%20Principles%20for%20Space%20Systems.pdf>; Matthew Scholl and Theresa Suloway, “Introduction to Cybersecurity for Commercial Satellite Operations,” NIST IR 8270 (National Institute of Standards and Technology, July 2023), <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8270.pdf>.
28. U.S. Department of Commerce, Bureau of Industry and Security, *Export Administration Regulations*, 15 C.F.R. pts. 730–774; “CLOUD Act Resources,” Department of Justice, accessed September 15,

- 2026, <https://www.justice.gov/criminal/cloud-act-resources>; National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, Version 1.0 (January 16, 2020).
29. Federal Communications Commission, *Report and Order and Further Notice of Proposed Rulemaking, Space Modernization for the 21st Century*, SB Docket No. 25-306, FCC 26-47 (July 22, 2026); *Licensing of Private Remote Sensing Space Systems*, 15 C.F.R. pt. 960.
 30. U.S. Department of Commerce, Bureau of Industry and Security, *Export Administration Regulations*, 15 C.F.R. pts. 730–774.
 31. Trump, “Space Policy Directive-5”; Scholl and Suloway, “Introduction to Cybersecurity for Commercial Satellite Operations.”
 32. Scholl and Suloway, “Introduction to Cybersecurity for Commercial Satellite Operations”; National Institute of Standards and Technology, “Software Security in Supply Chains” (May 5, 2022), <https://csrc.nist.gov/pubs/other/2022/05/05/software-security-in-supply-chains/final>.
 33. Bleier and Kumar, “Space Data Centers”; Beals, “Exploring a space-based scalable AI infrastructure system design.”
 34. “Data Center Demands,” McKinsey & Company, May 20, 2025, <https://www.mckinsey.com/featured-insights/charts/data-center-demands>; Bleier and Kumar, “Space Data Centers;” Howard, “Science & Tech Spotlight;” Noffsinger et al., “The Cost of Compute.”
 35. “Notice of Proposed Rulemaking, Spectrum Abundance for Weird Space Stuff,” SB Docket No. 26-54, FCC, March 27, 2026, <https://docs.fcc.gov/public/attachments/FCC-26-13A1.pdf>.
 36. “Report and Order and Further Notice of Proposed Rulemaking, Space Modernization for the 21st Century,” SB Docket No. 25-306, FCC, July 22, 2026; FCC, “Notice of Proposed Rulemaking, Spectrum Abundance for Weird Space Stuff.”
 37. *SAT Streamlining Act*, S. 3639, 119th Cong. (2026).
 38. Ellis Scherer, “Policy Reforms to Launch US Space Innovation” (ITIF, January 2026), <https://itif.org/publications/2026/01/05/policy-reforms-to-launch-us-space-innovation/>.
 39. *ORBITS Act*, S. 1898, 119th Cong. (2025), <https://www.congress.gov/bill/119th-congress/senate-bill/1898/text>; National Oceanic and Atmospheric Administration, “Traffic Coordination System for Space (TraCSS),” accessed August 12, 2026, <https://www.space.commerce.gov/traffic-coordination-system-for-space-tracss/>.
 40. National Aeronautics and Space Administration, “Orbital Debris Mitigation,” accessed August 12, 2026, <https://orbitaldebris.jsc.nasa.gov/mitigation/>.
 41. Trump, “Space Policy Directive-5”; Scholl and Suloway, “Introduction to Cybersecurity for Commercial Satellite Operations.”
 42. Scholl and Suloway, “Introduction to Cybersecurity for Commercial Satellite Operations”; National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0* (February 26, 2024), <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>.