



# National Spectrum Strategy

Comments Prepared for the National Telecommunications and Information Administration of the U.S. Department of Commerce

<p><b>Prepared for:</b> National Telecommunications and Information Administration U.S. Department of Commerce</p>	<p><b>Prepared By:</b> Matthew Zuccaro Director, Enterprise IT and Cybersecurity Frontier Foundry Corp.</p>
<p><b>RFI Information</b> Title: RFI in response to the Presidential Memorandum (PM), Modernizing United States Spectrum Policy and Establishing a National Spectrum Strategy</p>	
<p><b>Primary POC</b> Nick Reese COO and Co-Founder Frontier Foundry Corp. 8 The Green, Suite B Dover, DE 19901 Email: <a href="mailto:nickreese@frontierfoundry.com">nickreese@frontierfoundry.com</a></p>	





## Introduction

### **Background Information on Frontier Foundry**

Frontier Foundry Corp stands at the cutting edge of cybersecurity and artificial intelligence (AI), spearheading innovative solutions in these rapidly evolving domains. With a specialized focus on serving the banking, finance, government, and space domains, our organization combines deep technical expertise with a forward-thinking approach to address complex challenges in the digital realm. Our core strengths lie in developing robust cybersecurity frameworks and harnessing the power of AI to drive intelligent decision-making processes.

Our expertise extends to the intricate field of satellite cybersecurity. This niche specialization places us at the forefront of securing critical infrastructure in the space domain, an area increasingly pivotal to national and homeland security. Furthermore, our AI-driven solutions go beyond traditional security measures, offering innovative ways to optimize spectrum utilization and management, critical for efficient satellite operations.

### **Purpose of Response**

This response is crafted with the intention of contributing our insights and expertise to the National Spectrum Strategy. Recognizing the pivotal role of spectrum management in both national, homeland security, and commercial applications, particularly in the field of satellite communications, we aim to provide valuable recommendations that align with the Strategy's objectives. Our goal is to assist in shaping a spectrum environment that not only fosters technological innovation and economic growth but also ensures the highest standards of security and efficiency in spectrum usage. Drawing from our extensive experience in AI and cybersecurity, we are committed to offering solutions and perspectives that can help guide the Strategy towards achieving its long-term vision, especially in the context of evolving threats and technological advancements in the space sector.





## How the National Spectrum Strategy Impacts Us

The National Spectrum Strategy released by the Biden-Harris Administration, represents a comprehensive plan to modernize the United States' approach to spectrum policy. Key aspects of this strategy that align with Frontier Foundry's fields of expertise include:

- **Enhanced Satellite Communications:** The allocation of new spectrum bands and development of dynamic spectrum sharing technologies can greatly enhance satellite communication capabilities. This is particularly relevant for Frontier Foundry, whose focuses on satellite cybersecurity and applications for AI in the space domain would benefit from expanded and optimized spectrum usage.
- **Innovation in AI-driven Spectrum Management:** The Strategy's emphasis on AI for spectrum management opens new avenues for innovation in the satellite sector. AI can enable more efficient use of spectrum, predicting demand and optimizing bandwidth allocation, which is crucial for satellite operations.
- **Cybersecurity Implications:** With the expansion of spectrum usage, the importance of cybersecurity in protecting satellite communications infrastructure becomes paramount. Frontier Foundry's expertise in cybersecurity can contribute significantly to developing secure protocols and measures in this expanded spectrum environment.





## Focus Areas and Recommendations

### Secure Spectrum

Frontier Foundry advocates for continued research, development, and policy discussions on secure spectrum due to its applicability to support critical and emerging technologies, especially in the realm of space. Satellite communications, critical for both commercial and defense purposes, are becoming increasingly vulnerable to cyber threats. These threats range from signal jamming and interception to more sophisticated cyber-attacks aimed at controlling or damaging the on-orbit satellite vehicle and ground segment infrastructure. The introduction of secure spectrum should include the following considerations:

1. **Post-Quantum Cryptography:** Incorporating Post-Quantum Cryptography (PQC) should be considered as a forward-thinking strategy to ensure long-term security in the face of advancing quantum computing capabilities. PQC, designed to be secure against the potential threats posed by quantum computers, can be crucial in protecting the integrity of spectrum usage and management systems. For spectrum management, this means securing not just the data transmitted over the spectrum, but also the information and systems that manage and allocate the spectrum itself. As spectrum allocation becomes more dynamic and reliant on sophisticated algorithms, protecting these systems against quantum-level threats becomes imperative. PQC offers a layer of security that is resilient to both current and future decryption capabilities, ensuring that the control and access to spectrum resources remain secure from advanced computational threats. This approach to securing spectrum management systems with PQC is essential, especially as we move towards more interconnected and automated communication networks. By preemptively adopting post-quantum secure methods, the integrity and reliability of these crucial systems can be maintained, safeguarding against potential vulnerabilities that could arise with the advent of quantum computing technology.
2. **Spread Spectrum Technology:** Utilizing spread spectrum techniques, like Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS), can make signals less prone to interception and jamming.





These techniques spread the signal across a wider bandwidth, making it more difficult for unauthorized entities to isolate and disrupt the signal.

## Dynamic Spectrum

Dynamic spectrum sharing (DSS) allows for more efficient use of the available spectrum, especially in congested frequency bands. By enabling multiple users to access the same spectrum band without interference, it maximizes the utility of this scarce resource. DSS can improve connectivity and coverage for the sectors we work with, especially in banking and space such satellite communications, particularly in remote areas. As this technology evolves, Frontier Foundry strongly advocates for the creation of open-source advanced spectrum management tools aligned with the success of Open Radio Access Network (ORAN) technology. As the 6G standards process begins in earnest, effective and open-source spectrum management tools enabling a telecommunication standards that reflect democratic values. The concept of open-source development in advanced spectrum management tools, inspired by successful cybersecurity initiatives like MITRE's Cooperative Research and Development Agreement (CRADA), offers a transformative approach to addressing the challenges of DSS:

1. **Leveraging the CRADA Model:** The CRADA model, as pioneered by MITRE in cybersecurity, provides a collaborative framework where government agencies, private sector entities, and academic institutions work together. By adopting a similar approach for spectrum management, diverse expertise and resources can be pooled to develop more robust, innovative solutions.
2. **Standardization and Interoperability:** Developing open-source tools can also promote standardization across the satellite communications industry. This ensures interoperability between different systems and simplifies the process of integrating new technologies. Interoperability is a way to create increased security for the communications critical infrastructure sector.
3. **Government and Regulatory Support:** Advocacy for government support and funding for open-source spectrum management initiatives, much like the support MITRE received for cybersecurity advancements, can be crucial. This includes encouraging regulatory bodies to adopt and support these





tools, ensuring alignment with national and international spectrum policies.

## AI-driven Spectrum Management

In the realm of AI-driven spectrum management, the provision of open-source, non-synthetic training data is pivotal. Open-source training data sets play a crucial role in the development and refinement of AI models used in spectrum management. They enable AI algorithms to learn from a diverse and comprehensive range of scenarios, enhancing their accuracy and reliability. This is particularly important in the dynamic and complex field of spectrum management, where AI systems must adapt to a wide variety of signal environments and interference patterns. For AI-driven spectrum management, particularly in the context of dynamic spectrum sharing and satellite communications, the type of data needed for open-source training is quite specific and diverse. Here are some key categories of data that would be essential:

1. **Spectrum Usage Data:** Historical and real-time data on spectrum usage across various bands and geographic locations. This includes data on frequency, bandwidth, duration, and intensity of spectrum usage by different types of users (e.g., commercial, governmental, satellite).
2. **Interference Data:** Information about past and present interference incidents in the spectrum, including the types of interference (e.g., accidental overlap, deliberate jamming), their sources, frequencies affected, and the impact on communication systems.
3. **Signal Characteristics:** Data on the characteristics of different types of signals used in satellite communications, including modulation types, signal strength, bandwidth requirements, and propagation models.
4. **Environmental Data:** Information on how various environmental factors (like weather conditions, topography, urban vs. rural settings) affect spectrum propagation and usage. This is particularly relevant for satellite communications, where signal transmission can be impacted by atmospheric conditions.



## Policy and Regulatory Recommendations

Our recommendations aim to address key areas where education, international collaboration, and a nuanced understanding of the geopolitical landscape can significantly influence the effective and equitable use of spectrum resources. These recommendations, while diverse in their focus, share a common goal: to enhance global communication capabilities, foster international cooperation, and ensure that spectrum management remains a tool for technological advancement and global connectivity, rather than a point of contention in geopolitical rivalries.

### 1. Educating Public Stakeholders on the Importance of Spectrum

- **Objective:** Raise awareness about the critical role of spectrum in various aspects of modern life, from communication to navigation and beyond.
- **Implementation:** Develop and provide free curriculum tools for educational institutions, particularly targeting secondary schools. This curriculum should cover the basics of spectrum technology, its applications, and its importance in everyday technology.
- **Benefits:** Educating young minds not only fosters a deeper understanding of technology but also inspires future innovation. An informed public is better equipped to engage with and support policies that promote effective spectrum management.

### 2. Increased Engagement and Training with International Partners, especially in the Global South

- **Recognition:** Frontier Foundry commends the efforts of the NTIA's International Affairs team and the United States Telecommunications Training Institute (USTTI) in their ongoing international engagement and training initiatives.
- **Strategy:** Expand these efforts to focus more on partnerships with countries in the Global South. This could involve more targeted training programs, knowledge-sharing initiatives, and collaborative projects focused on spectrum management.
- **Impact:** Strengthening global cooperation in spectrum management is essential, especially for developing countries where spectrum-related infrastructure and regulatory frameworks are still evolving. This can lead to





more harmonized global spectrum management practices and bridge the digital divide.

### 3. Recognizing the Politicization of Global Spectrum Allocation and Standards

- **Challenge:** Acknowledge that the technocratic role of global spectrum allocation has increasingly become a matter of geopolitical interest, particularly in the context of the emerging great power rivalry between the US and the People's Republic of China.
- **Approach:** Advocate for maintaining a balanced and scientifically driven approach to global spectrum management. This involves recognizing and navigating the political aspects while striving to keep spectrum allocation decisions grounded in technical efficacy, fairness, and global cooperation.
- **Importance:** In an era where technology is often intertwined with geopolitical interests, it's crucial to advocate for policies that prioritize global connectivity and technological advancement, while being mindful of the broader political landscape. Balancing these interests is key to ensuring that spectrum management remains a tool for global development and cooperation, rather than a point of contention.





## About the Team

Frontier Foundry is a data and artificial intelligence company focused on combining unrivaled domain expertise with creative implementations of AI. Our team has expertise in integrating complex datasets to extract meaningful insights as well as customizing AI algorithms to specific industry needs, ensuring both accuracy and practical applicability.

### **Sultan Meghji, CEO and Co-Founder**

Sultan Meghji most recently served as the inaugural Chief Innovation Officer at the Federal Deposit Insurance Corporation of the United States Government, prior to becoming the Co-Founder and CEO of Frontier Foundry Corp. A noted expert in AI, Biotech, Cybersecurity, Quantum Computing & Web3, he also serves as a scholar at the Carnegie Endowment for International Peace, a fellow at the George Mason National Security Institute and is a distinguished member of the Bretton Woods Committee. Mr. Meghji also serves as a professor in the graduate programs at Duke University's Pratt Engineering School with a focus on AI, Web3 & Cybersecurity.

### **Nick Reese, COO and Co-Founder**

Nick Reese is the Cofounder and COO of Frontier Foundry Corp. Nick most recently served as the first ever Director of Emerging Technology Policy at the US Department of Homeland Security where he advised the White House and senior Cabinet officials on national security implications of emerging technologies. He is the author of the DHS AI Strategy and the lead DHS representative for the development of Space Policy Directive-5, National Security Memorandum-10, the National Space Policy, and Executive Order 13960. Mr. Reese has a 20+ year career in the US Military, Intelligence Community & Homeland security with a focus on operations and bringing technical solutions to high stakes national security challenges.

### **Dr. Jimmie Lenz, Principal, Advanced Research**

Dr. Lenz is the Director of the Master of Engineering in FinTech and the Master of Engineering in Cybersecurity at the Pratt School, teaching Machine Learning and Blockchain. He has a secondary appointment as the Irene and Frank Salerno Visiting Professor of Financial Economics, and leads the Digital Asset Research





and Engineering Collaborative (DAREC). Dr. Lenz holds an undergraduate degree from the University of South Carolina, a Master of Science in Finance from Washington University in Saint Louis, and Doctor of Business Administration-Finance from Washington University's Olin Business School.

### **Dr. Roque Martinez, Senior Vice President of Technology**

Dr. Roque Martinez is a technology executive renowned for his hands-on approach to delivering advanced software solutions in multifaceted environments. Throughout his career, he has consistently demonstrated a visionary aptitude, both in formulating long-term strategies and in realizing immediate tactical objectives. Dr. Martinez holds a Doctor of Business Administration from Rutgers Business School, where he delved into machine learning and performance prediction using startup financial models.

### **Matthew Zuccaro, Director, Enterprise IT and Cybersecurity**

Matthew Zuccaro orchestrates the technological harmonies at Frontier Foundry Corp as the Director of Enterprise IT & Cybersecurity. In college, Matt would have majored in Lego Architecture if that was an option but instead settled on a BA (summa cum laude) in history, where he focused on dissecting the long term policy implications of the United States Government from 1945 to 1980. After a stint in entrepreneurship, Matt finally put his public policy experience to work at the U.S. Department of State, where he focused on cybersecurity, telecommunications, counternarcotics, and bridging the digital divide. Matt comes to Frontier Foundry with a wealth of practical hands-on experience and a tenacious passion for all-things digital. When not at work, or playing catch with his sons, Matt enjoys traveling, model railroading, and of course, Legos!

