Request for Information:
Small Satellite Cybersecurity Testbed Mission

30 April 2026

The Aerospace Corporation
HEADQUARTERS:
14745 Lee Road
Chantilly, VA 20151

TECHNOLOGY CAMPUS:
2310 E. El Segundo Blvd.
El Segundo, CA 90245-4609

The Aerospace Corporation UK Ltd
Suite 5, Adam House
7-10 Adam Street
The Strand
London, WC2N 6AA, United Kingdom
contact@aerospacecorp.uk

Respondent's role in the Organization/Points of Contact:
(US Contact) Pamela S. Wood, Senior Project Leader pamela.s.wood@aero.org
(UK Contact) Dave Sandy, Managing Director david.sandy@aerospacecorp.uk

Respondent Type: *Federally Funded Research and Development Center (FFRDC)*

THE AEROSPACE CORPORATION
TECHNOLOGY CAMPUS:
2310 E. El Segundo Blvd.
El Segundo, CA 90245-4609
www.aerospace.org

REQUEST FOR INFORMATION (RFI)

Small Satellite Cybersecurity Testbed Mission
Issuing Organization: Aerospace UK in partnership with Aerospace US
Issue Date: 30 April 2026
Response Deadline: 29 May 2026
Classification: UNCLASSIFIED

---

1. INTRODUCTION AND PURPOSE

1.1 Background

The Aerospace Corporation United Kingdom (UK) Ltd (Aerospace UK) in partnership with The Aerospace Corporation (Aerospace) is seeking information from qualified industry partners regarding the design, development, and procurement of an on-orbit cybersecurity testbed platform. This platform shall consist of a secure space vehicle (bus) hosting a cyber payload designed to support the development of defensive cyber operations (DCO), cyber tactics, techniques, and procedures (TTPs), and enable end-to-end verification of cyber-related kill chains across the space enterprise.

This voluntary RFI builds upon previous cybersecurity space mission concepts (see Appendix A) and seeks to understand current industry capabilities for delivering an integrated platform that provides either (or both) a secure, operationally reliable spacecraft and a representative, reconfigurable cyber payload suitable for experimentation and training.

Success of a program of this type resembles a flexible, innovative solution towards providing a platform that furthers the development, experimentation, and demonstration of cybersecurity related solutions for the space domain with the maximum amount of realism possible. There is no prescribed design beyond the need to operate the space vehicle safely and responsibly during the entirety of the program, but use of the space vehicle subsystems and/or telemetry for cybersecurity experiments is reasonable. A vendor can provide part or all the solutions sought.

1.2 Objectives

The primary objectives of this RFI are to:

- Assess industry capabilities for rapid development and procurement of cybersecurity testbed satellite platforms
- Understand current state-of-the-art in secure-by-design spacecraft architectures that can host vulnerable cyber payloads
- Gather information on design approaches for representative, operationally relevant cyber testbed payloads
- Identify potential partners with relevant experience and heritage in both secure systems and cyber testbed development
- Understand cost, schedule, and risk considerations for integrated platform procurement
- Understand and explore partnership opportunities with members of the space industry

1.3 Reference Mission Concept

Respondents should consider a mission concept similar to the following baseline for the on-orbit cybersecurity testbed platform:

- **Form Factor:** Minimum 3U CubeSat, maximum 12U (larger platforms acceptable with extra volume utilization explanation)
- **Mission Duration:** 3-year operational life (goal: 5+ years)
- **Orbit:** LEO, 400-590 km altitude, various inclinations acceptable
- **Platform Architecture:**
  - Secure space vehicle bus with heritage subsystems
  - Hosted cyber payload with COTS/representative components
  - Dedicated onboard hardware to provide secured and supervised connection between bus and experimental cyber payload
  - Capability to reset/restore payload without compromising bus
- **Ground Segment:** Secure ground operations with external participant access capabilities
- **Mission Participants:** Government, industry, academic, and, potentially, public participants

---

2. SCOPE OF INFORMATION REQUESTED

2.1 Organizational Capabilities and Experience

2.1.1 General Information

- Company name, location(s), and organizational structure
- Years in business and number of employees
- Security clearance capabilities (if applicable)
- Previous government contracting experience
- Quality certifications (ISO 9001, AS9100, etc.)

2.1.2 Space Mission Heritage

- Number and types of spacecraft developed and launched
- CubeSat/SmallSat specific experience (quantity, form factors, mission types)
- On-orbit performance record and lessons learned
- **Mission longevity experience:** Examples of missions achieving 3+ years operational life
- Examples of rapid development programs (e.g., ATP + 24 months)
- Experience with experimental or technology demonstration missions
- Flight heritage of bus subsystems proposed for this mission

2.1.3 Secure-by-Design Experience

- **Critical:** Describe your organization's experience with secure-by-design principles in spacecraft development
- Approaches to cybersecurity in space system architecture

- Experience implementing security controls in resource-constrained environments
- Methodologies for threat modeling and security requirements development
  Experience with security testing, vulnerability assessment, and penetration testing
- Approaches to supply chain security and component verification
- Examples of systems designed with security isolation/segmentation
- Experience with secure boot, cryptographic implementations, or secure communications
- Experience designing secure platforms that host experimental or potentially vulnerable payloads

2.1.4 International Partnership Experience

- **Critical:** Characterize your organization's experience working with international customers by country/region, with particular emphasis on:
  - United States (U.S.) government or commercial entities
  - United Kingdom (UK) government or commercial entities
  - Other US Allied nations (NATO, Five Eyes, etc.)
- Understanding of relevant export control regulations and compliance frameworks (ITAR, EAR, UK export controls, etc.)
- Experience navigating international technology transfer and data sharing agreements
- Previous international collaborative space missions
- Capabilities for supporting international participants in mission operations
- Experience with multinational exercise or training environments

2.2 Technical Approach and Design Considerations

2.2.1 Spacecraft Bus Design (if applicable to your response)

- Proposed spacecraft architecture and form factors for the secure space vehicle
- Heritage and maturity of bus subsystems:
  - Command and Data Handling
  - Electrical Power System
  - Attitude Determination and Control System
  - Thermal Control
  - Structures and Mechanisms
  - Propulsion (if applicable)
- Redundancy and fault tolerance approaches
- Radiation tolerance and component selection philosophy for 3-5+ year missions
- Software architecture and operating system
- Approach to establishing secure and supervised connection between bus and experimental cyber payload and prioritizing independence of critical bus functions from hosted cyber payload
- Bus monitoring and safing capabilities

THE AEROSPACE CORPORATION
TECHNOLOGY CAMPUS:
2310 E. El Segundo Blvd.
El Segundo, CA 90245-4609
www.aerospace.org

2.2.2 Cyber Payload Design Philosophy (if applicable to your response)

- **Critical:** Approach to designing a representative cyber payload hosted on the secure bus
- Strategy for creating operationally relevant cyber-attack surfaces
- Proposed payload components and rationale (processors, radios, sensors, etc.)
- Approach to payload reconfigurability and software updates
- Methods for isolating cyber payload from critical bus functions while maintaining operational realism
- Capability to reset/restore payload to known states without affecting bus
- Data logging and forensics capabilities
- Balance between security and experimental accessibility
- Interface design between secure bus and cyber payload

2.2.3 Communications Architecture (if applicable to your response)

- Proposed RF communications approach (frequencies, data rates, ground networks)
- Strategy for secure command and control of the space vehicle bus
- Approach to providing external participant access to cyber payload while protecting critical bus functions
- Experience with commercial ground networks (e.g., KSAT, AWS Ground Station)
- Encryption and authentication methodologies
- Separation of operational (bus) and experimental (payload) communications paths

2.2.4 Ground Segment Design (if applicable to your response)

- Ground system architecture for mission operations of the integrated platform
- Approach to multi-user access with varying privilege levels
- Cloud infrastructure considerations and security
- Data management and distribution strategies
- Interface design for external participants (red team/blue team access to payload)
- Secure operator access to bus functions
- Compliance with government cybersecurity frameworks (NIST, RMF, etc.)

2.2.5 Mission Operations Concept

- Proposed CONOPS for cyber experimentation using the hosted payload
- Approach to exercise planning and execution
- Safety protocols, rules of engagement, and responses to protect the space vehicle
- Telemetry, tracking, and commanding philosophy for both bus and payload
- Anomaly response and recovery procedures
- Support for various exercise types (training, competitions, research)
- Approach to maintaining platform availability and reliability over 3-5+ year mission

2.3 Quality Assurance and Software Assurance

2.3.1 Quality Control Processes

- **Critical:** Quality management system overview
- Configuration management approach for integrated platform
- Parts, materials, and processes (PMP) control
- Nonconformance tracking and resolution
- Testing philosophy and test coverage
- Environmental testing capabilities and approach
- Acceptance criteria and success metrics
- Quality approach for both secure bus and cyber payload components

2.3.2 Software Development and Assurance

- **Critical:** Software development lifecycles and methodologies
- Software quality assurance processes
- Code review and testing practices (unit, integration, system)
- Software verification and validation approach
- Version control and configuration management
- Flight software update and patching capabilities for both bus and payload
- Approach to managing different security postures between bus and payload software

2.3.3 Vulnerability Testing and Security Validation

- **Critical:** Processes for security testing during development
- Vulnerability assessment methodologies
- Penetration testing capabilities and approach
- Security validation at component, subsystem, and system levels
- Third-party security assessment experience
- Continuous monitoring and security operations capabilities
- Testing approach to verify isolation between secure bus and cyber payload

2.4 Schedule Considerations

2.4.1 Development Timeline Options

Please provide estimated timelines for the following scenarios for delivering the complete on-orbit cybersecurity testbed platform:

- **Rapid Development:** Maximum urgency, accepting higher risk
- **Regular Development:** Balanced approach to schedule, cost, and risk
- **Relaxed Development:** Lower risk, more thorough verification

For each scenario, identify:

- Major milestones and reviews (PDR, CDR, TRR, etc.)
- Critical path items

- Long-lead procurement items
- Integration and test duration for complete platform
- Delivery to launch integrator timeframe

2.4.2 Procurement Lead Times

- **Critical:** Typical lead times for major subsystems and components
- Supply chain risks and mitigation strategies
- Component obsolescence considerations for 3-5+ year missions
- Strategies for schedule compression
- Impact of export control on procurement timelines

2.5 Cost Information

2.5.1 Cost Estimates

Please provide rough order of magnitude (ROM) cost estimates for the complete on-orbit cybersecurity testbed platform:

- Spacecraft bus (flight unit + engineering model/flatsat)
- Cyber payload development (flight unit + flatsat)
- Integrated platform assembly, integration, and test
- Ground segment development and operations (first year)
- Launch integration support
- Mission operations (per year)
- Program management and systems engineering
- Identify major cost drivers and potential cost reduction opportunities

2.5.2 Cost-Schedule-Risk Trades

- Discussion of cost implications for different schedule approaches
- Impact of requirements changes on cost and schedule
- Risk mitigation costs
- Opportunities for cost sharing or international collaboration

2.6 Risk Considerations

2.6.1 Technical Risks

- Identification of major technical risks for this integrated platform concept
- Proposed mitigation strategies
- Technology readiness levels (TRL) of proposed components
- Heritage vs. new development trade-offs
- Risks associated with hosting cyber payload on secure bus
- Mission longevity risks for 3-5+ year operations

2.6.2 Programmatic Risks

- Schedule risks and mitigation approaches
- Supply chain and vendor risks
- Export control and international partnership risks
- Launch availability and integration risks

2.6.3 Security Risks

- Risks associated with creating intentionally vulnerable payloads on secure platforms
- Insider threat considerations
- Supply chain security risks
- Operational security risks during cyber exercises
- Risk of payload compromise affecting bus operations

---

3. ADDITIONAL INFORMATION OF INTEREST

3.1 Innovation and Advanced Concepts

- Novel approaches to cyber testbed platform design
- Emerging technologies applicable to this mission
- Innovative ground segment or operations concepts
- Ideas for enhancing mission value or expanding capabilities
- Approaches to extending platform life beyond 5 years

3.2 Lessons Learned

- Key lessons from previous small satellite programs
- Common pitfalls in rapid development efforts
- Insights from cybersecurity-related space missions
- Recommendations for mission success
- Lessons learned from long-duration small satellite missions

3.3 Partnership and Collaboration

- Interest in teaming arrangements
- Complementary capabilities with other organizations
- Proposed role in potential mission (prime, subcontractor, partner)
- Experience with government-industry-academic partnerships

3.4 International Collaboration Considerations

For all respondents—Characterization of Customer Experience:

- Identify any restrictions on working with specific international partners
- Describe approach to managing multi-national programs

- Experience with:
  - U.S. government customers (DoD, NASA, NRO, Intelligence Community, etc.)
  - UK government customers (MOD, GCHQ, UK Space Agency, etc.)
  - other U.S. Allied nation customers
- Understanding of applicable security and export control frameworks
- Capabilities for supporting exercises involving U.S. and Allied participants
- Regulatory considerations for international collaborative missions
- Opportunities for US-Allied collaboration models
- Supply chain considerations for international partnerships

---

4. RFI RESPONSE INSTRUCTIONS

4.1 Response Format

- Maximum page limit: 30 pages (excluding cover page and table of contents)
- Format: PDF, 12-point font minimum, 1-inch margins
  Include table of contents with section references
- Number all pages
- Clearly mark any proprietary or competition-sensitive information

4.2 Response Structure

Responses should address the sections outlined in Section 2 in order. Use clear headings and subheadings. Provide specific examples and quantitative data where possible.

4.3 Submission Instructions

Submit responses electronically to: Pamela.S.Wood@aero.org

Subject line: "RFI Response—Small Satellite Cybersecurity Testbed—Aerospace UK"

4.4 Questions and Clarifications

Questions regarding this RFI should be submitted in writing to Pamela.S.Wood@aero.org no later than 30 May 2026. Responses to questions will be provided to all parties who have registered interest in this RFI.

4.5 Points of Contact

Pamela S Wood (US Contact)
Senior Project Leader
Vehicle Autonomy, Safety and Trust Department
The Aerospace Corporation
Pamela.S.Wood@aero.org
+1-571-304-3908

Dave Sandy (UK Contact)
Managing Director
The Aerospace Corporation UK Ltd.
David.Sandy@aerospacecorp.uk
+44-774-971-7788

5. IMPORTANT NOTICES

5.1 Nature of This Request

This is a Request for Information (RFI) only. This RFI is issued solely for information and planning purposes and does not constitute a solicitation. No contract will be awarded based on responses to this RFI. Responses will be used to inform potential future procurement strategies for an on-orbit cybersecurity testbed platform.

5.2 No Commitment

Responses to this RFI are voluntary. Aerospace UK is under no obligation to award a contract, issue a solicitation, or provide funding as a result of this RFI. Respondents will not be reimbursed for costs incurred in preparing responses.

5.3 Proprietary Information

While respondents are encouraged to provide detailed information, they should clearly mark any proprietary or competition-sensitive information. Aerospace UK will protect such information to the extent permitted by law but cannot guarantee absolute confidentiality.

5.4 No Organizational Conflicts of Interest

Responses to this RFI may be used to inform requirements development and acquisition strategy of various government organizations. Organizations that provide substantial support in these areas may be precluded from competing for subsequent implementation contracts due to organizational conflicts of interest.

5.5 Export Control

Respondents are responsible for ensuring their responses comply with all applicable export control regulations. Do not include controlled technical data in RFI responses without proper authorization.

5.6 Evaluation

Responses will be evaluated to assess:

- Relevance and depth of experience
- Technical approach viability for integrated platform
- Understanding of mission requirements
- Capability to execute within reasonable cost and schedule constraints
- Innovation and value-added capabilities
- Approach to balancing secure bus with experimental payload

This RFI does not establish a competitive range, and all interested parties are encouraged to respond.

THE AEROSPACE CORPORATION
TECHNOLOGY CAMPUS:
2310 E. El Segundo Blvd.
El Segundo, CA 90245-4609
www.aerospace.org

APPENDIX A: REFERENCE DOCUMENTS

THE AEROSPACE CORPORATION
TECHNOLOGY CAMPUS:
2310 E. El Segundo Blvd.
El Segundo, CA 90245-4609
www.aerospace.org

The following documents are provided as reference for a previous similar mission concept:

- Moonlighter Fact Sheet: https://aerospace.org/fact-sheet/moonlighter-fact-sheet
- Air Force Research Laboratory (AFRL) Hack-a-Sat: https://afresearchlab.com/hack-a-sat/
- Moonlighter FCC Mission Statement: https://apps.fcc.gov/els/GetAtt.html?id=307212

These documents illustrate one approach to a cybersecurity testbed mission but should not constrain innovative alternative approaches. Respondents should feel free to propose different technical solutions that meet the overall mission objectives for an integrated on-orbit cybersecurity testbed platform.

THE AEROSPACE CORPORATION
TECHNOLOGY CAMPUS:
2310 E. El Segundo Blvd.
El Segundo, CA 90245-4609
www.aerospace.org

APPENDIX B: ACRONYMS AND DEFINITIONS

THE AEROSPACE CORPORATION
TECHNOLOGY CAMPUS:
2310 E. El Segundo Blvd.
El Segundo, CA 90245-4609
www.aerospace.org

ACB - Attitude Control Board

ACS - Attitude Control System

ADCS - Attitude Determination and Control System

CDR - Critical Design Review

CONOPS - Concept of Operations

COTS - Commercial Off-The-Shelf

DCO - Defensive Cyber Operations

EAR - Export Administration Regulations

EPS - Electrical Power System

ITAR - International Traffic in Arms Regulations

LEO - Low Earth Orbit

PDR - Preliminary Design Review

RFI - Request for Information

ROM - Rough Order of Magnitude

SOE - Statement of Expectations

TRL - Technology Readiness Level

TRR - Test Readiness Review

TTP - Tactics, Techniques, and Procedures