Attachment Request for Information
Biosurveillance and Biological Detection Capabilities

BACKGROUND:

The biological threat environment to the U.S. homeland continues to evolve. Biological threats include naturally occurring pathogens, and biological agents that have been enhanced through biotechnology including advances in synthetic biology. Coupled with globally connected transportation systems, increasingly complex operational environments, and the growing accessibility of advanced biological capabilities, there is value in reimagining the technologies needed to protect the American public and those sworn to protect them.

The Department of Homeland Security Science and Technology Directorate is exploring novel biosurveillance, biological detection, anomaly detection, and biological characterization capabilities that may support homeland security missions involving:

- Early warning
- Threat detection
- Situational awareness
- Biological event characterization
- Operational decision support
- Response coordination
- Risk assessment

The Department is also interested in exploring these capabilities that integrate Artificial Intelligence-driven analytics, machine learning, and high-performance. These capabilities should aid in homeland security operational missions including but not limited to:

- Safeguarding the health of the American people and our economy through:
    - Infrastructure resilience
    - Border and transportation security
    - Maritime security
    - Public safety operations
    - Emergency and incident management
    - Disaster preparedness and response
    - Critical infrastructure protection

Previous biodetection and biosurveillance efforts have demonstrated the importance of:

- Reducing false positives (i.e., specificity) and operational burden
- Improving timeliness of detection and validation (e.g., sensitivity)
- Integrating heterogeneous data sources to provide context for decision-making
- Supporting operationally actionable decision-making
- Maintaining flexibility to include emerging threats including novel or engineered biological threats
- Accelerating laboratory confirmation timelines
- Enabling scalable and interoperable architectures
- Collecting evidence and maintaining chain of custody to support forensic attribution

Attachment Request for Information
Biosurveillance and Biological Detection Capabilities

The Department of Homeland Security Science and Technology Directorate recognizes that biosurveillance architectures will likely require biological sensing, meterological analysis, anomaly analytics, field screening, nucleic acid or peptide sequencing, laboratory validation, mobility data, epidemiological indicators, operational analytics, and decision-support systems operating across multiple biological pathways and operational environments.

The Government is interested in technologies, operational concepts, architectures, workflows, and integrated approaches capable of supporting domestic biosurveillance and biological awareness missions.

The Government is also interested in capabilities relevant to airborne, environmental, waterborne, foodborne, vector-borne, human, animal, agricultural, maritime, transportation-related, and other biologically relevant operational pathways.

PURPOSE:

This Request for Information solicits information regarding current, emerging, developmental, or operational capabilities relevant to homeland security biosurveillance and biological detection missions.

The Department of Homeland Security Science and Technology Directorate seeks information regarding capabilities supporting:

- Detection and identification of known or unknown biological threats, including emerging pathogens and biological threat agents enhanced or enabled by biotechnologies including synthetic biology
- Detection and identification of unknown or anomalous biological activity
- Integrated biosurveillance and situational awareness
- Rapid methods to confirm detection of a biological incident and provide useful insight on the incident (e.g., virulence markers, antimicrobial susceptibility or resistance, phylogenetic relationships, other characteristics and corroborating signals) at or near the point of detection
- Biological incident risk analytics that support operational response
- Scalable and interoperable biosurveillance ecosystems

The Government is particularly interested in capabilities capable of operating under conditions involving:

- Dynamic population movement
- Incomplete or delayed information
- Adversarial manipulation to include obfuscation
- Complex operational environments
- Collecting and preserving evidence to support forensic investigation

The Department of Homeland Security is not limiting this Request for Information to aerosolized biological detection systems or traditional environmental biodetection architectures.

Attachment Request for Information
Biosurveillance and Biological Detection Capabilities

The Government is interested in both individual technologies and integrated capability approaches spanning environmental, clinical, population-level, operational, agricultural, veterinary, transportation, border, maritime, and infrastructure-related biological monitoring domains. This includes advanced sensing, detection, characterization, anomaly recognition, validation, and decision-support capabilities, as well as architectures capable of integrating multiple technologies, data sources, and operational workflows.

The Government recognizes that biosurveillance and biological awareness missions may require layered, interoperable, and adaptive approaches operating across multiple operational environments and biological pathways.

CAPABILITY AREAS OF INTEREST

The Department of Homeland Security is interested in technologies and approaches relevant to one or more of the following capability areas:

1. Detection of Known Biological Threats

Capabilities designed to detect, identify, and characterize known biological agents and threat materials.

Potential capabilities may include, but are not limited to:

- Multi-domain biological sampling and collection in operational environments
- Multi-domain biological sensing technologies, such as:
    - Polymerase Chain Reaction (PCR) and molecular detection
    - Sequencing platforms
    - Immunoassays
    - Mass Spectroscopy including Matrix-Assisted Laser Desorption/Ionization Time-of-Flight (MALDI-TOF) technologies
- Environmental and biological sensing systems
- Multi-domain biological collection and sensing systems
- Portable confirmatory detection
- Autonomous biological monitoring systems

2. Detection of Unknown or Anomalous Biological Activity

Capabilities designed to identify abnormal biological conditions without requiring prior knowledge of a specific agent or predefined signature library.

Potential capabilities may include, but are not limited to:

- Host-response detection and diagnostics tools
- Environmental anomaly detection
- Artificial Intelligence / Machine Learning (AI/ML)-enabled biological signal recognition
- Genomic divergence analysis
- Wastewater biosurveillance analytics

- Syndromic surveillance approaches
- Multi-signal biosurveillance fusion
- Novel pathogen detection approaches
- Population-level anomaly and trend analysis

3. Integrated Biosurveillance and Situational Awareness

Capabilities supporting biological awareness and operational decision-making through integrated data and analytic environments.

Potential capabilities may include:

- Artificial Intelligence / Machine Learning anomaly analytics
- Federated data fusion
- Cross-domain signal correlation
- Predictive outbreak analytics
- Human-in-the-loop alerting
- Operational dashboards
- Shared situational awareness tools
- Operational risk scoring systems
- Distributed biological analytics
- Decision-support environments

Potential data sources may include one or more of the following:

- Wastewater indicators
- Clinical indicators
- Syndromic surveillance
- Transportation and mobility data
- Border and travel indicators
- Environmental monitoring
- Public safety indicators
- Emergency call center indicators
- Veterinary indicators
- Agricultural indicators
- Supply-chain indicators
- Infrastructure disruption indicators
- Genomic surveillance

4. Rapid Validation and Characterization

Capabilities designed to reduce delays associated with centralized laboratory dependency and confirmatory analysis.

Potential capabilities may include:

- Portable sequencing
- Mobile laboratory systems

- Rapid field assays
- Distributed and field-deployable detection and diagnostics including at point of testing
- Automated, or no, sample preparation
- Distributed validation architectures
- Autonomous validation systems
- Cartridge-based confirmation systems
- Artificial Intelligence-assisted biological validation
- Mobile characterization units
- Biological fingerprinting systems

The Department of Homeland Security is particularly interested in approaches that accelerate operational confidence and characterization at or near the closest operational point to detection.

5. Scalable and Interoperable Biosurveillance Ecosystems

Capabilities supporting interoperable biosurveillance architectures.

Potential areas of interest include:

- Open architectures
- Application Programming Interface (API) compatibility
- Modular system design
- Federated analytics
- Cloud and edge integration
- Cybersecurity and resilience of biosecurity architectures
- Data standards
- Human-machine teaming
- Replay and simulation capabilities
- Synthetic data environments
- Decision traceability
- Explainable Artificial Intelligence approaches

RFI QUESTIONS:
The following questions will help the Department of Homeland Security Science and Technology Directorate better understand the current state of the market, operational feasibility, technical maturity, deployment considerations, and future opportunities relevant to biosurveillance and biological detection capabilities.

Other pertinent information may be provided in addition to responses to the questions below.

1. Company or organization information, including name, address, phone number, email, point of contact, and website Uniform Resource Locator (URL).

2. Describe the biological detection, biosurveillance, anomaly detection, validation, or biological awareness capability being proposed.
3. What operational problem does the capability address?
4. What biological threats, conditions, or indicators can the capability detect, characterize, monitor, or assess?
5. Is the capability:
    - signature-based,
    - agent-agnostic,
    - anomaly-based,
    - or hybrid?
6. Describe the primary technical approach, architecture, and concept of operations.
7. What data sources are required or integrated?
8. Has the capability been operationally demonstrated or field tested?
9. What is the current Technology Readiness Level (TRL)?
10. What is the state of the technology (i.e. established, prototype, or planned enhancements/emerging, etc.)?
11. What environmental or operational conditions can the capability tolerate?
12. What are the false positive and false negative characteristics?
13. What operational limitations currently exist?
14. What level of operator skill or specialized training is required?
15. What bandwidth, compute, storage, cloud, or communications dependencies exist?
16. Does the capability support edge operation, disconnected environments, or degraded communications environments?
17. Can the capability detect or characterize previously unknown, engineered, or emerging biological threats?
18. Can the capability provide near-laboratory-grade validation or characterization in the field?
19. What is the timeline from initial detection to actionable operational confidence?
20. How does the capability reduce or eliminate centralized laboratory dependency?
21. Can validation or characterization occur autonomously or at the closest operational point to detection?
22. How are uncertainty, confidence, and operational risk communicated to operators and decision-makers?

23. Does the capability support interoperability with public health, Laboratory Response Network (LRN), emergency management, or homeland security operational systems?
24. What cybersecurity protections are incorporated?
25. What Application Programming Interfaces, interoperability standards, or data exchange formats are supported?
26. What deployment, sustainment, and maintenance considerations exist?
27. What are the primary technical, operational, or programmatic risks associated with deployment?
28. What are the Rough Order of Magnitude (ROM) deployment and sustainment costs?
29. What partnerships, infrastructure, or external dependencies would be required to operationalize the capability at scale?
30. If properly resourced, how quickly could the capability be deployed operationally?
31. What future research, development, testing, or operational experimentation activities would most accelerate maturation of the capability?
32. What is the nature of the current supply chain? What would an ideal future supply chain look like.

RESPONSE GUIDELINES & REQUIRED FORMAT:

Sources will not be reimbursed for providing responses.

Responses to this Request for Information should be no more than twenty (20) typewritten pages and should be prepared in either Microsoft Word (.doc or .docx) or Adobe Acrobat (.pdf) formats.

Responses should be prepared using:

- 12-point font
- 1-inch margins
- 8.5” x 11” page format

This includes images, charts, diagrams, tables, and figures.

Responses should include:

- Organization name
- Technical and management points of contact
- Email address
- Telephone number
- Relevant technical materials

- Architecture diagrams or workflows (if available)
- Relevant operational demonstrations or testing information

ADDITIONAL INFORMATION:

All information received will be treated as market research information and may be used in Department of Homeland Security Science and Technology Directorate program documentation, strategic planning, technology assessments, operational experimentation planning, architecture development, requirements analysis, and future acquisition planning activities.

Proprietary information submitted as part of responses should be clearly marked and identified as PROPRIETARY.

The Government reserves the right to hold one-on-one meetings, technical exchanges, demonstrations, or follow-up discussions as part of its market research activities.

QUESTIONS:

The Government will not provide answers to questions on this RFI.

DUE DATE:

The due date for the submission of responses to this RFI is 5:00 PM Eastern Time on June 5, 2026. Responses shall include "**RFI - 70RSAT26RFI000019 - Biosurveillance and Biological Detection Capabilities"** in the subject and sent via email to the following address: opoindustryliaison@hq.dhs.gov