PRIISM™: Secure SaaS for Full Spectrum Targeting and Multi-Domain C2

30 January 2026

Proposal Submitted By:
Research Innovations Incorporated
6363 Walker Lane STE 500
Alexandria, VA 22310

Table of Contents

1.0 Company Overview

Research Innovations Incorporated (RII) is a mission-focused technology company dedicated to solving complex planning and data challenges for the public sector. RII's United Kingdom (UK) business specialises in developing advanced software solutions for the UK Ministry of Defence, national security, and allied government partners. Our agile, user-centred approach, combined with a team of embedded operational subject matter experts, allows us to rapidly deliver mission-critical capabilities that help commanders and planners make better, faster decisions.

2.0 Value Proposition

RII provides a proven, Technology Readiness Level (TRL) 7 digital workspace that unifies operational planning, coordination, and execution. Unlike legacy systems that create data silos, PRIISM™ operates as a node within your federated data fabric, ingesting data from disparate sensors and systems to create a single, real-time version of the truth. Validated in large-scale coalition command post exercises, PRIISM acts as the "decide" system for the headquarters, enabling commanders to make data-driven decisions at the speed of relevance.

We specialise in "Software Defined" warfare, delivering capabilities faster than traditional procurement cycles. RII engineers have proven the ability to deploy code updates to the tactical edge within 24 hours, rapidly parsing new message formats and fixing interoperability breaks in the field. This agility ensures the software evolves in real-time alongside the threat, rather than waiting for distant release cycles.

PRIISM eliminates vendor lock-in through a Modular Open Systems Approach (MOSA). We actively collaborate with the wider defence ecosystem, functioning as the "connective tissue" between hardware and software providers. The platform has successfully integrated tracks from third-party artificial intelligence sensor fabrics and uncrewed systems to automate multi-vendor kill chains. We open our Application Programming Interfaces (API) and share data models to ensure seamless interoperability with sovereign UK systems and United States (US) command networks.

Our delivery capability is grounded in deep domain expertise. RII's UK team is comprised of military veterans, ensuring that our software is designed by people who understand the user's reality. This operational empathy translates to measurable efficiency gains: in recent trials, PRIISM demonstrated a 75% reduction in sensor-to-decider timelines and a tenfold increase in execution capacity by removing manual data entry steps.

PRIISM solves issues by providing a unified, secure, and configurable Software as a Service (SaaS) environment that implements Mission Applications (MA) and other optional capabilities aligned with UK doctrine:

- **PRIISM Decision Advantage** serves as a unified digital workspace for military planning, coordination, and synchronisation. It directly enables Integrated Action by providing tools to orchestrate effects across domains aligned with the commander's intent. By streamlining planning processes supporting both the tactical estimate and combat estimate, PRIISM enhances situational awareness and fosters shared understanding, contributing to Decision Advantage.
- The **PRIISM Joint Targeting Platform (PRIISM JTP™)** module operationalises UK Full Spectrum Targeting policy. It supports the entire Targeting Cycle, from target development and

validation to capability analysis, decision support, mission planning, and assessment. PRIISM JTP facilitates rigorous Target List Management (TLM) and ensures accountability through decision capture, Target Engagement Authority (TEA) recording, and audit trails suitable for Target Clearance Boards (TCB). It enables synchronization of deliberate and dynamic targeting, including Time-Sensitive Targets (TST).

- The **PRIISM Information Advantage Platform** is a web-based Information Operations (Info Ops) mission support product that helps defence teams understand audiences and the information environment, plan and synchronise information activities, manage messaging and product workflows, route outputs through configurable approvals (including policy, Operational Security (OPSEC) and Personnel Security (PERSEC), and log delivery and effects for assessment and reporting. It supports audience-centric planning by linking intent, outcomes, activities, and measures in one place, enabling deconfliction across Media Operations, Psychological Operations (PsyOps) and Engagement, with audit trails and exportable outputs for governance and lessons. It can ingest governed Publicly Available Information (PAI) and Commercially Available Information (CAI) to inform analysis and assessment, supports role-based access controls, and can be deployed in secure environments including disconnected or air-gapped networks, with customer-owned data and interoperability through open interfaces and exports.
- **PRIISM Integrated Network (PRIISM-IN)** is a solution for Network Operations (NetOps) and Command and Control (C2). Built on a MOSA it provides a single interface for teams of NetOps personnel to visualize and coordinate diverse assets from the tactical edge to higher echelons. The scalable NetOps offers automated discovery and real-time health visualization of the network. This ensures networks are actively managed and adapted in real-time, providing commanders the agility and resilience required for multi-domain operations in contested environments, contributing to decision advantage.
- Our optional Generative Artificial Intelligence (Gen AI) capability, powered by Large Language Models (**LLM),** enhances planning and decision-making within PRIISM by processing complex text and data inputs. It accelerates steps within the tactical estimate and Combat Estimate (CE), such as Intelligence Preparation of the Environment (IPE), threat evaluation, mission analysis, Course of Action (COA), development and analysis/wargaming, and assessment against Measures of Effectiveness / Measures of Performance (MOE/MOP). This accelerates the Assess-Decide-Direct cycle, contributing to decision advantage.

Key outcomes for buyers include:

- **Proven Lethality:** In recent exercises, PRIISM reduced the Sensor-Decider-Effector (SDE) chain from 12 minutes to 3 minutes and increased target execution capacity tenfold (from 25 to 250 targets per hour).
- **Improved Tempo:** Shorten planning cycles through standardised workflows.
- **Better Accountability:** Gain transparent audit through decision capture and versioned artefacts.
- **Increased Coordination:** Improve alignment of activities, authorities, and effects to lines of operation.

3.0 What the Service Provides

PRIISM is a secure, supplier-hosted SaaS environment for military planning, coordination, and situational awareness. It serves as a unified digital workspace, enabling defence organisations to ingest data from diverse sources, manage workflows, and maintain a single version of the truth aligned with the Common Operating Picture (COP).

The environment provides the following in scope core capabilities:

- **Unified Digital Workspace:** Centralised environment for operational planning and coordination aligned to UK doctrine.
- **Data Fabric Ingestion:** Native ingestion of structured data via API, including Cursor-on-Target (CoT) and US Message Text Format (USMTF)
- **Role-Based Access Control (RBAC):** Granular permission management ensuring users only access data appropriate to their role and clearance.
- **Configurable Workflows**: Standardised user journeys for approvals, governance, and decision logging without bespoke code
- **Automated Reporting:** Configurable dashboards and reports for real-time status tracking and post-operational analysis
- **Secure Hosting:** Hosted on MODCloud infrastructure as a cloud environment (iACE) with Interim Authority to Operate (IAtO) for OFFICIAL-SENSITIVE
- **Interoperability:** Validated integration with widely used C2 systems via RESTful APIs and open standards
- **Audit and Logging:** Comprehensive immutable logging of all user actions and decision points for accountability and operational analysis
- **Open Data Standards:** Data exportable in non-proprietary formats (JSON, CSV, XML, Apache Parquet) to prevent vendor lock-in
- **Resilient Architecture:** Designed for high availability with automated backup schedules and disaster recovery protocols

Optional SaaS MA/modules/features available under this listing include:

- **PRIISM Joint Targeting Platform (PRIISM-JTP):** Extends core with target development, nomination, list management, approval routing, and effects tracking capabilities. Available as the primary application within a Full Licence (Item L2-4) or as an add-on for existing instances (Item L2-MA)
- **PRIISM Information Advantage Platform (PRIISM-IA):** Enables decision superiority over competitors by integrating cyber protection and “inform, influence, attack” activities across staff functions, echelons, and coalition partners. Available as the primary application within a Full Licence (Item L2-4) or as an add-on for existing instances (Item L2-MA)
- **PRIISM Integrated Network (PRIISM- IN):** Provides NetOps and C2 monitoring. Available as the primary application within a Full Licence (Item L2-4) or as an add-on for existing instances (Item L2-MA)
- **LLM Capability:** Provides AI assistance for planning, COA analysis, and assessment integrated within the workflows. This is a consumption-based service configured with a set amount of tokens per deployment, as specified in the Pricing Document (Item L2-16).
- **Exercise Support**: This is scoped as a surge of effort to deploy a team to support an exercise or event over a period of time for integration at an exercise or lab risk reduction, etc., and produce a final report. Available as an add-on (Item L2-15)
- **Small, Medium, or Large Solution Modules** - These correspond to the fixed-price solution packages listed in the Pricing Document. They provide scoped effort for business process integration, configuration, and legacy capability migration. Available as an add-on (Item L2-4/5/6)

We also include as optional add-ons:

- **Solution Modules and Support Packages:** Provide a means for user organisations to obtain custom integration, command, or function specific modules that ease the integration from an organisation's localised and self-maintained set of capabilities into the PRIISM environment that provide increased value to their organisations and processes through enterprise-scale solutions in secure cloud architectures enabling big data capabilities..
- **Systems Integration & Data Migration:** Assistance with integrating PRIISM into buyer environments, large-scale data migration, and custom connector development.
- **Enhanced Training:** Tailored training programmes are offered as part of the Consultancy & Support (L2-18) offering, 'train the trainer' courses, and ongoing user enablement beyond the standard SaaS onboarding.
- **Managed Operations & Support:** Options for 24/7 support are offered as part of the Ancillary Services (L2-19) offering, extended service level agreements (SLAs), on-call services, and supplier-managed operations within the buyer's environment.
- **Custom Reporting:** Development and delivery of bespoke reporting packs tailored to specific buyer needs. These reports are offered under the “Experimentation Staff Support (L2-15) or “Consultancy & Support (L2-18) offerings.
- **Consultancy & Support:** Staff augmentation, consultancy, discovery workshops, change management support, and strategic advice related to cloud adoption and optimisation.

The Base (250 user) and Trial (75 user) licences include access to one primary MA of the buyer's choice (e.g. PRIISM JTP or PRIISM IA).

Buyers requiring simultaneous access to multiple MAs (e.g. both Targeting and Information Operations) must purchase the “MA-Access” add-on for each additional application required.

Configuration Limits and Assumptions

- Configuration through the UI (forms, fields, stages, roles, dashboards, report templates) is in scope.
- API access is in scope where published in technical documentation.

Data Ingestion and Export Boundaries

- **In scope:** Data import via UI upload and published APIs from approved sources; schema mapping using in-product tools where provided.
- **In scope:** Export of user owned data and audit logs in documented formats.

Service Boundaries and Dependencies

- Accessed via a secure browser session (supported versions in technical section).
- Single Sign On (SSO) supported with compatible buyer Identity Provider (IdP) and metadata.
- Buyer responsible for network allow listing and DNS changes on their networks.

Pricing and Licensing Alignment

- The service is procured via a block licence model, providing a set capacity of users: Full Licence (Item L2-1): Up to 250 users for a 12-month term. Trial Licence (Item L2-2): Up to

75 users for a 12-month term. Exercise Licence (Item L2-3): Up to 25 users for a fixed 4-month term to support short-duration events or experiments.

4.0 Typical Users and Buyers

4.1 Target Organisations

The service is intended for UK defence and public sector organisations that need to plan, coordinate, and assess operations and information activities in a controlled environment. Typical contracting entities include central government departments and defence organisations and agencies. Where applicable, other public sector bodies with resilience, emergency management, or public information functions may also use the service.

Typical buyers and stakeholders

- Senior Responsible Owner (SRO) and programme leads: outcomes, governance, spend approval.
- Service owners and product managers: adoption, configuration, service management.
- Information assurance and security teams: risk management, access control, audit and logging, compliance.
- Commercial and procurement staff: scope, pricing, call-off terms.
- Operational leads (planning, targeting, information operations, engagement): day-to-day direction and prioritisation.
- Technical administrators: user management, tenant configuration within product settings, access reviews.

User roles (personas) and primary tasks

- **Planners and coordinators:** build and manage plans, align activities to lines of operation, track dependencies, generate briefs, and handover packs
- **Targeting staff:** develop and manage target lists, capture authorities, route approvals, record effects and assessments
- **Information operations teams:** plan and track information activities, align messages to audiences, assess performance and impact
- **Analysts:** ingest approved data, maintain reference sets, produce dashboards and reports, support assessments
- **Engagement leads and liaison officers:** plan and record engagements, deconflict activity, capture outcomes and follow-ups
- **Command staff:** review status, risks and decisions, approve artefacts, direct resources
- **Administrators:** manage users, roles and least-privilege profiles, configure forms, stages and dashboards, oversee audit and continuity tasks
- **Licence types (published pricing)**
  Licences map to user needs so buyers can scale by function. The Pricing Document lists inclusions and any volume discounts that apply uniformly to all buyers.
- **Viewer:** read-only access to views, dashboards and reports; export where permitted by role
- **Standard User**: full create/update within assigned workflows, target list interactions where enabled, report generation and exports
- **Advanced/Planner:** all Standard rights plus configuration of team views, saved filters, templated reports and workflow stages within allowed boundaries
- **Administrator:** tenant administration, role management, baseline configuration, audit access

- **Optional Mission Application access:** rights to PRIISM JTP, PRIISM IN, and the Gen AI capability are assigned per user according to the buyer's licence mix and appear as add-on entitlements in the Pricing Document

Testing approach: combination of automated scans, manual keyboard only testing, screen reader testing, contrast and focus order checks, and user journey reviews for key tasks; accessibility regressions checked during release cycles; issues tracked to resolution in the supplier's defect system

Documentation: admin and user guides provided in accessible formats; headings, landmarks, and alt text applied; captions provided for training media where applicable

Data protection and role mapping note. Access is role-based and aligned to least privilege. Buyers designate a named "administrator" to manage role assignments and to ensure licence allocation matches user duties.

5.0 Outcomes and Deliverables

Outcomes (enabled by PRIISM):

1. **Faster planning and coordination:** PRIISM supports shorter planning and coordination cycles by using configurable workflows, shared workspaces, and standardised artefacts and views.
2. **Governance and accountability:** PRIISM supports decision traceability through approval chains, decision capture, version control, and activity logging, with exportable audit logs where required.
3. **Consistent reporting for briefings, handover, and assessment:** PRIISM supports dashboarding and templated reporting aligned to buyer objectives, with secure export for handover or analysis.

Deliverables:

1. **Provisioned service access:** buyer access to a secure, supplier-hosted PRIISM environment via a web browser.
2. **Baseline configuration:** initial configuration within the UI, including forms, fields, workflow stages, roles, dashboards, and report templates (within documented configuration limits).
3. **Access control set up:** RBAC and least-privilege profiles, with single sign-on support where the buyer provides a compatible identity provider.
4. **Data import and export within scope:** import via UI upload and published application programming interfaces from approved sources, and export of user-owned data and audit logs in documented formats.
5. **Onboarding and offboarding:** provisioning to first login, baseline configuration support, data export options, and secure deletion on request.
6. **Documentation and standard support access:** access to product documentation and standard support channels as defined in the 8.0 Service Management and Support section.

6.0 Ordering, Onboarding, and Implementation

This section describes the process from placing an order through to users accessing the configured PRIISM service.

6.1 Ordering and Invoicing

This section describes the process from placing an order through to users accessing the configured PRIISM service.

Ordering

PRIISM is ordered through the Government Cloud (G-Cloud) call-off process using the published pricing for licence types and any optional modules selected by the buyer. The buyer specifies: Number of user licences by type (Base, Trial, Exercise).

1. MAs to be enabled within the service (for example PRIISM JTP, PRIISM IN, optional Gen AI capability).
2. Any optional add-ons included in the call-off (for example onboarding package, training modules, support tier).

Ordering is completed using the standard G-Cloud Call-off Order Form and associated call-off terms.

Invoicing

Invoices are paid fully upfront or in accordance with a milestone schedule.

Sustainment and Renewals: Buyers renewing existing PRIISM SaaS contracts should refer to the Sustainment and Support options (Items L2-10 through L2-12) in the Pricing Document. These items provide for the recurring maintenance of MAs and core software, including system administration and accreditation maintenance. Specific licence renewals are priced at the standard rates listed in items L2-1 through L2-3 unless otherwise agreed in the Call-Off Contract.

6.2 Implementation Plan

A detailed implementation plan, tailored to the buyer's specific requirements, can be provided on request following contract award.

A standard onboarding plan is provided at contract start. Onboarding provides a guided path from call-off start to first login and baseline configuration within the product.

Typical onboarding steps:

1. **Call-off validation**
   Confirm call-off details, buyer contacts, named administrator, licence mix, selected optional modules, and agreed onboarding outputs.
2. **Tenant provisioning**
   Provision the buyer tenant and apply the agreed baseline configuration within product settings, including initial administrator access.
3. **Authentication configuration**
   Configure authentication based on the buyer environment and agreed approach. This may include integration with a buyer identity provider for SSO where applicable.

4. **Role and permission set-up**
   Apply least-privilege roles aligned to buyer duties and enable module entitlements according to the buyer's licence mix.
5. **Workspace configuration**
   Configure workspaces, fields, workflow stages, and approval routes using in-product tools. Load buyer-provided reference data where required and permitted.
6. **Onboarding handover**
   Confirm support channels, provide onboarding documentation, and complete administrator handover.

Data Import (within SaaS Scope)

In scope data import includes:

1. Import via the UI and published API using supported formats and schemas.
2. Schema mapping using in-product configuration tools where available.
3. Standard validation checks (for example required fields, data types, and schema compliance). Failures are reported back to the buyer for correction and re-import.

Out of scope:
The following are not included in this Lot 2b SaaS listing:

1. Buyer-specific Extract, Transform, Load (ETL) development
2. Data cleansing and transformation services
3. Large-scale data migration activities
4. Custom connector development and integration work beyond published interfaces

Timescales & Dependencies

- **Lead Time:** Typical time to first login is within 10 to 15 UK business days of receiving complete buyer inputs IdP metadata, admin details, licence choices, reference data
- **Buyer Dependencies:** Timely provision of IdP metadata/test accounts, nominated administrators/role mappings, and any reference data is required from the buyer.

Acceptance Criteria

Onboarding is considered complete when:

- Buyer administrators can authenticate via SSO and access admin functions.
- Representative users can authenticate and perform agreed test tasks in enabled modules.
- Baseline configuration and roles are documented and approved by the buyer.
- Support channels are confirmed and operational.

Responsibilities

Supplier responsibilities

1. Provision the tenant and apply baseline configuration within product settings.
2. Configure authentication according to the agreed approach.

3. Apply RBACs aligned to least privilege.
4. Provide standard guidance for data import within published interface constraints.
5. Deliver standard onboarding training and administrator handover.
6. Confirm support routes and incident reporting process.

Buyer responsibilities

1. Provide identity and authentication details and test accounts where applicable.
2. Nominate administrators and confirm role mapping and access decisions.
3. Provide reference data required for baseline configuration where applicable.
4. Validate configuration outputs and confirm acceptance.
5. Manage internal rollout, user communications, and organisational change.

6.3 Training

Standard user and administrator training is included within the onboarding process to facilitate orientation to the service:

- **Quick Start Guides:** Links provided to concise user and admin guides in accessible formats.
- **User Onboarding Session:** A session (approx 60-90 minutes) covering login, navigation, roles, core workflows, search, dashboards, reporting, and data export.
- **Administrator Handover Session:** A more detailed session (approx. 90+ minutes) covering user/role management, configuration options, audit access, and support procedures.

Additional enhanced training modules can be met via the additional Support Services options.

6.4 Support During Onboarding

Standard support is available during UK business hours throughout the onboarding period via our normal support channels (detailed in Section 10).

Exit Readiness Established at Onboarding

Data export options, request routes, and formats are explained during the administrator handover, ensuring the buyer understands exit choices from the start.

7.0 Offboarding and Exit

7.1 Overview

Buyers retain ownership of their data at all times. The service supports export of buyer data in common, documented formats during the contract and at exit. Deletion is only performed on written instruction from the buyer's authorised contracting authority.

7.2 What Can Be Exported

Buyer data stored in the buyer's service instance (tenant), including:

- Records and reference data created or uploaded by users

- Attachments in their original file formats
- Configuration items created within the product (for example: workflows, fields, dashboards), where export is supported
- Audit and event data:
    - Administrative and user activity logs relevant to governance and compliance review
    - Export can be scoped by time period, user set, and object type to support least-privilege disclosure.

When exports can be requested: Exports can be requested at any time during the contract period and during the agreed exit window following contract end.

7.3 Export Methods and Formats

Self-service export (role-permitted users)

- Common data objects can be exported directly to:
    - Comma Separated Values (CSV)
    - Microsoft Excel (XLSX)
    - JavaScript Object Notation (JSON)

Ticketed full export (buyer request via support): A complete export package for the buyer's tenant can be produced by the supplier and delivered securely.

Packaging

- Tabular data: CSV and/or XLSX
- Structured objects: JSON with documented structures
- Attachments: original file formats plus a CSV or JSON manifest linking files to records
- Audit logs: CSV or JSON including actor, action, timestamp, object affected, and outcome

7.4 Export Service Levels

Self-service exports initiated by users are produced immediately or near real time, subject to data volume.

Ticketed full export: Target delivery within 5 UK business days of receiving a complete request, subject to data volume and an agreed delivery schedule.

Secure delivery: Export packages are delivered via an agreed secure method, for example:
Secure File Transfer Protocol (SFTP) to a buyer endpoint, or a buyer-provided secure file exchange platform.

7.5 Deletion and Retention

Buyer-controlled deletion: Data deletion is performed only on written instruction from the buyer's authorised contracting authority, typically after the buyer confirms successful receipt of the final export (or explicitly waives export).

Retention period after contract end: Buyer data is retained for a defined period after contract termination to support export completion and validation. The retention period is stated in the order form or call-off schedules (including exit management terms) for the specific call-off.

Deletion method and evidence: Deletion follows an auditable process appropriate to the storage media and hosting model. On request, the supplier will provide a deletion certificate stating the tenant identifier, scope of deletion, method, dates, and authorising personnel.

Backups: Backups containing buyer data follow the supplier's backup retention schedule. Where deletion is instructed, backups expire and are permanently removed in line with that schedule.

7.6 No Vendor Lock-in

1. **Open formats** Exports use common formats (CSV, XLSX, JSON) with documented structures to support migration to other tools or repositories.
2. **No proprietary reader required** No proprietary software is required to access exported files and attachments.
3. **Clear exit process** Roles, timelines, export options, and validation steps are provided to the buyer administrator during onboarding and in the administration guide.

Roles and responsibilities at exit: Exit strategy documentation including a full Responsible, Accountable, Consulted and Informed (RACI) matrix will be exchanged post contract.

Change control during exit: To maintain export consistency, the parties may agree to a short change-freeze window for the final export (for example: read-only access). Any freeze will be scheduled during UK business hours and communicated in advance.

8.0 Service Management and Support

This section outlines the service levels, support arrangements, and maintenance procedures applicable to the PRIISM SaaS platform provided under this Lot 2b listing. Any enhanced support, managed services, or bespoke reporting fall outside this scope and are available separately under our additional Support Services listings.

8.1 Service Levels

- **Target Availability:**
  - The service target availability is 95%[1] per calendar month, measured at the service edge.
  - Included components for availability measurement are authentication, core application services, and published APIs.

- **Incident Management:**
  - **Priorities (Examples):**

[1] *As previously advised, a 95% availability target (allowing over 36 hours of potential downtime per month) is significantly below market expectation (typically 99.5% or 99.9%) for an operational service and presents a major risk to your bid. Strongly recommend revising this upwards.*

- **P1 Critical:** Complete service unavailability or significant data loss in progress; confirmed major security incident.
- **P2 High:** Major feature/module unavailable for many users with no reasonable workaround.
- **P3 Medium:** Degraded performance or defect with a reasonable workaround available.
- **P4 Low:** Minor defect, cosmetic issue, or documentation query.

8.2 Service Constraints

- **Support Hours:**
  - Standard support for this service is available 09:00 to 17:00 UK time, Monday to Friday, excluding UK public holidays.
  - Enhanced support options (e.g extended hours, 24x7 cover) are available.
- **Support Channels:**
  - Buyers can raise support requests via email. A phone number is available for P1 Critical incidents.
- **Planned Maintenance Window:**
  - Standard planned maintenance is scheduled with 72 hours' notice.

8.3 Outage and Maintenance Management

- **Availability Measurement & Exclusions:**
  - Availability is calculated as the percentage of total minutes in a calendar month the service is fully available, excluding planned maintenance within the declared window; buyer or third-party issues (e.g identity provider outage, local network problems); force majeure events; significant volumetric attacks beyond reasonable supplier control.
- **Status Communications:**
  - Service status updates and incident notifications are provided via the Defence Digital (DD) Forward Schedule of Change and direct email notifications to named buyer administrators.
- **Emergency Maintenance:**
  - Carried out only for critical security or stability fixes. Notice will be provided as soon as is practicable, which may be after the event for urgent issues. Expected impact is typically brief interruption.
- **Change Control and Release Management:**
  - **Cadence:** Regular minor software releases occur quarterly; maintenance releases are scheduled within the planned maintenance window.
  - **Compatibility:** APIs and core user journeys aim to remain backward compatible where feasible. Breaking changes are avoided or carefully managed.
  - **Notifications:** Release notes detailing changes affecting functionality, roles, permissions, or security are sent to buyer administrators before deployment. Emergency changes are communicated post deployment.
- **Incident Communications & Closure:**
  - Support requests receive acknowledgement with an incident ID and assigned priority.
  - A Post-Incident rReport (PIR) detailing root cause, timeline, and corrective/preventive actions is provided for P1 and P2 incidents within 5 UK business days of resolution.

9.0 Technical and Service Requirements

This section outlines the technical prerequisites for accessing the PRIISM service and the responsibilities that the buyer must fulfil.

9.1 Technical Requirements

To access and use the PRIISM SaaS, the buyer's environment must meet the following requirements:

- **Client Access:** Users access the service via a secure web browser session. Supported modern desktop browsers include Google Chrome, Microsoft Edge, and Mozilla Firefox. Browser versions are listed in the detailed technical documentation.
- **Network Connectivity:** Buyer networks must allow outbound HTTPS connections on port 443 to the designated PRIISM service endpoints. Specific Internet Protocol (IP) addresses or domain names for allow-listing will be provided during onboarding. The buyer is responsible for making any necessary Domain Name System (DNS) or firewall changes on their network.
- **Authentication (SSO):** The service supports SSO integration.

9.2 Customer Responsibilities

The buyer is responsible for the following to ensure successful service delivery and use:

- **Provide Information for Setup:** Supply necessary details for SSO configuration, including identity provider metadata and test user accounts. Provide names and contact details for designated administrator(s). Supply any buyer specific reference data (e.g. audience sets, lines of operation) required for initial configuration loading.
- **User and Access Management:** Provision user identities within their identity provider system for SSO access. Manage the user lifecycle (joiners, movers, leavers) within their own systems. Designate administrator(s) responsible for managing role assignments within PRIISM to ensure licence allocation matches user duties and adheres to the principle of least privilege.
- **Configuration and Validation:** Provide timely validation of configuration decisions during onboarding and any subsequent changes.
- **Local Environment Management:** Maintain the availability and correct configuration of their identity provider service. Manage their local network infrastructure, including firewalls and DNS settings. Ensure users have access via supported web browsers.
- **Incident Reporting:** Report service incidents promptly via the specified support channels, providing sufficient diagnostic detail to aid investigation.
- **Internal Communications:** Communicate user rollout plans and manage any internal change management processes related to adopting the service.

9.3 Development Life Cycle of the Solution

The PRIISM SaaS platform is developed and maintained using an Agile methodology. We operate a regular release cadence for delivering minor feature updates, enhancements, and security patches. Maintenance releases are typically deployed within the planned maintenance window. Changes are managed to maintain backwards compatibility where feasible, and release notes are provided to buyer administrators ahead of deployment.

10.0 Security and Data Protection

10.1 Data Locations and Sovereignty

- **Primary Hosting:** The PRIISM service is hosted within MODCloud iACE, utilising Microsoft Azure Platform as a Service (PaaS) components.
- **Data Residency:** All core processing and storage of buyer data occurs within approved UK regions.
- **Data Transfer:** Buyer data does not move outside these approved UK regions, except where necessary for using approved sub-processors explicitly listed in the Data Processing Agreement (DPA).

10.2 Classification Posture

- **Scope:** This service listing is designed and assured for information classified up to OFFICIAL, including data handled with OFFICIAL-SENSITIVE caveats by the buyer.
- **Above OFFICIAL:** Deployment or operation at classifications above OFFICIAL is outside the scope of this Lot 2b SaaS offering and would require separate procurement, hosting, and assurance arrangements.
- **Handling Guidance:** Users authenticate using MOD-approved methods (e.g. PKI) over secure HTTPS/TLS connections. Unauthenticated access attempts do not reveal system information. The buyer's specific operational policies govern the handling and content classification within the application, whereby all data objects stored must be appropriately marked with a security classification label by the user or system upon ingest.

10.3 Access Control

- **Authentication:** Access requires positive authentication using the buyer's designated identity provider, typically integrated via SSO using Public Key Infrastructure (PKI) client certificates. The service validates the presented certificate; access is denied without a valid certificate.
- **Authorisation:** The service employs multiple layers of authorisation checks, including Policy-Based Access Control (PBAC) for system-wide and per-record sharing rules, RBAC defining access to applications/objects/data based on user roles, Rule-Based Access Control (RuBAC) applying boolean logic based on data attributes (e.g.review status), and Mandatory Access Control (MAC) enforcing security markings (like classification) down to the data storage level .
- **Least Privilege:** Access is granted based on predefined roles aligned with the principle of least privilege.
- **Administrative Safeguards:** Privileged administrator roles (Application and System Administrators) are distinct from standard user roles. Separation of duties is enforced, requiring privileged users to maintain separate accounts for standard and administrative tasks. All administrative activity is audited.
- **Session Management:** User sessions automatically time out after a defined period of inactivity.

10.4 Audit and Logging

- **Scope:** The service logs key events, including authentication attempts (success/failure), administrative actions (e.g. user management, configuration changes), data import/export operations, key workflow actions (e.g. approvals, decisions), and significant user activities. Logs include timestamps synchronised via Network Time Protocol (NTP), actor identity, action performed, object affected, and outcome. Data Provenance records are also maintained for data elements.
- **Retention:** Audit logs are retained for 7 years

- Buyer Access: Buyers can view selected audit events within the application interface. A full export of audit logs relevant to the buyer's tenant is available upon request via a support ticket (refer to Section 7.0 Offboarding and Exit).

10.5 Encryption and Key Management

- **In Transit:** All external access to the service (UI and APIs) is encrypted using HTTPS/Transport Layer Security (TLS 1.2 or higher) on port 443. Internal service-to-service communication is also secured using TLS.

10.6 Backups and Disaster Recovery

- **Backup Schedule:** Core datasets undergo automated backups, including full backups every 24 hours and database table level backups every 4 hours, with automated rolling retention.
- **Disaster Recovery Testing:** Disaster recovery procedures, including data restoration from backups, are tested at a defined frequency. Evidence of the last successful test date is available upon request.
- **Restore Process:** Data restoration can be initiated via a support ticket by named buyer administrators and is typically scheduled during UK business hours.

Assurance

- **Accreditation:** While the core PRIISM platform maintains a baseline IAtO on MODCloud, buyers with unique data handling requirements or distinct risk appetites may require a dedicated accreditation effort.
- **Supplier Security:** RII management devices used for administrative access operate under corporate security controls, maintaining Cyber Essentials Plus certification, and using Virtual Private Networks (VPN), Endpoint Detection & Response (EDR)/Extended Detection & Response (XDR) tools, and disk encryption.

10.7 Vulnerability Management

- **Baselines and Scanning:** Security baselines derived from sources like Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG-) and Security Requirements Guides (SRG-) are applied where applicable. Automated tools like the Assured Compliance Assessment Solution (ACAS) are used for compliance checks and vulnerability scanning before deployment.

- **Patching:** Patches are applied according to a defined policy based on severity. Target timelines are: we have 30 days on Critical and 90 days on High with a POAM (Plan to address in a release)
- **Penetration Testing:** Independent security testing, such as Infrastructure Testing Health Checks (ITHC), is performed periodically annually in line with accreditation activities.

10.8 Sub-Processors

- **Usage:** The service uses approved sub-processors primarily for hosting (Microsoft Azure) and potentially other operational functions.
- **Governance:** All sub-processors are vetted and bound by contractual agreements, including the DPA, which includes appropriate safeguards if data is processed outside the UK/EEA.

10.9 Incident Reporting and Breach Response

- **Detection and Escalation:** Service health and security alerts are monitored continuously. Pre-defined procedures (runbooks) dictate escalation paths for different incident types.
- **Buyer Notification:** In the event of a confirmed personal data breach, RII will notify Buyer without undue delay (pursuant to Joint Schedule 10). For any unlawful access to or loss of Buyer content in cloud platforms, RII will notify Buyer within 48 hours (pursuant to the Framework Special Terms). For a security incident, the RII will notify Buyer within 24 hours (pursuant to the Security Schedules 9A-9E). Further, RII will assist the Buyer in meeting its regulatory notification obligations.
- **Report Contents:** Initial notification includes known facts, potential scope, and mitigation steps, with regular updates provided until resolution. Follow-up reporting will include a Breach Action Plan (BRP) within 5 working days, as required. This report will include full details of the breach (a summary, timeline, affected systems/data [where known]), a root cause analysis, remedial actions taken, and preventative measures implemented.
- **Notification Channels:** Notifications are sent to named Buyer administrators via email. If there is a breach involving Personal Data, RII may undertake communication or engagement activities with the affected individuals. P1 Critical security events may also trigger phone contact.

10.10 Operational Security Controls

- **Production Access:** Access to production environments is strictly limited to authorised personnel using role-based least privilege. All access is logged. Privileged users operate separate administrative accounts.
- **Environment Segregation:** Development, pre-production, and production environments are logically and/or physically separated. Production data is not used in lower environments without explicit approval and appropriate data sanitisation or masking controls.
- **Business Continuity Communications:** Service status information and operational communications are maintained during incidents and planned maintenance periods.

11.0 Privacy and GDPR

11.1 Roles and Responsibilities

- **Controller/Processor:** Buyer acts as Data Controller and RII acts as Data Processor for personal data processed by the service.

- **Joint controllership**: The service is not designed for joint-controller arrangements. If any processing requires joint controllership (e.g. shared determination of purposes), this will be documented in writing before enablement, including roles, decision rights and contact points.
- **Sub processing:** RII may use sub-processors for hosting and specific operational functions as listed in the DPA annex; RII remains responsible for sub processor performance and compliance.

11.2 Data Processing Agreement (DPA)

- **Basis:** processing governed by a DPA aligned to UK GDPR and the Data Protection Act 2018, incorporating Article 28 processor obligations
- **Standard terms:** link to supplier DPA provided in the call-off pack
- **International transfers:** RII understands that it may not transfer Personal Data outside of the UK without the Buyer's prior written consent and ensuring appropriate safeguards are in place. Should processing involve non-UK/EEA locations, appropriate safeguards are applied (e.g. International Data Transfer Agreement (IDTA) or EU SCCs with the UK Addendum).
- **Sub-processor changes:** Buyer written consent will be obtained prior to engaging in new sub-processors for personal data. RII will ensure that they are bound by equivalent contractual data protection obligations as RII, noting that RII normally does not engage with any sub-processors who are not GDPR-compliant.

11.3 Data Categories and Purpose

- **Typical personal data:** user identifiers (name, email, role/organisation), authentication and authorisation events, usage and configuration metadata, and audit logs.
- **Operational content:** records and documents uploaded or created by users may contain personal data depending on buyer use. The buyer is responsible for ensuring data minimisation and lawfulness of content entered into the system.
- **Special category data:** the service is not intended for systematic processing of special category data. Where buyers choose to process such data for operational reasons, they must establish a lawful basis and appropriate policy documents/controls; the service provides access control, logging and encryption to support buyer compliance.
- **Children's data:** not intended for processing personal data relating to children.

11.4 Data Subject Rights (DSR)

- **Supported rights:** access, rectification, erasure, restriction, portability and objection, subject to legal/operational exemptions determined by the Controller.
- **Handling model:**
    - The Controller receives and validates the request.
    - The Controller may fulfil the request using in-product tools (search, export, update, delete) where available.
    - Where supplier action is required, the Controller raises a ticket; the supplier acts only on the Controller's documented instruction.
    - Timeframes: the supplier supports the Controller to meet statutory timelines (normally one month from receipt); complex requests may be extended in line with UK GDPR.
    - Identity and scope: the Controller is responsible for requester identity verification and for defining the dataset/scope of each request.

12.0 Privacy by Design and Default

Data minimisation features: configurable roles and least-privilege profiles; optional masking/redaction patterns via configuration where supported.

Logging and accountability: administrative and user actions are logged; audit exports available to support investigations and compliance reviews.

Pseudonymisation/anonymisation: supported through Buyer processes and data-handling practices; the service does not automatically anonymise operational content. Additionally, with the IA Mission application, the platform integrates a secure IP anonymisation service to mask user traffic when accessing public media sites, protecting operator attribution and digital signatures during external research activities.

12.1 Retention and Deletion

- **Retention configuration:** buyers define retention in line with their policies. Where system-level defaults apply (e.g. audit log retention), values are documented in the Security section and the Admin Guide.
- **End-of-contract:** on contract termination, the buyer may request a full export and instruct secure deletion. Backups age out per the documented backup retention schedule before being permanently removed (see Section 7.0 Offboarding and Exit).
- **Legal holds:** on written request from the Controller, deletion may be suspended for specified datasets to meet legal or regulatory requirements.

12.2 Lawful Basis and Transparency

The Controller determines the lawful basis for processing and informs data subjects as required. As Processor, RII provides information about technical and organisational measures to support the Controller's transparency obligations. Should RII consider that any of the Controller's instructions infringe on GDPR, it will notify the Controller immediately.

12.3 Security of Processing (Summary)

Personal Data is protected by encryption in transit and at rest, access control, and monitoring as detailed in Section 10.0 Security and Data Protection. The supplier ensures that persons authorised to process personal data are subject to confidentiality obligations.

12.4 Breach Notification

RII will notify the Buyer (Controller) without undue delay after becoming aware of a confirmed personal-data breach, sharing initial facts, likely consequences and measures taken or proposed, and will assist the Controller in meeting regulatory notification duties, as described above in Section 10.10 Incident Reporting and Breach Response.

Controller contact: nominated by the Buyer at call-off.

Data locations and sovereignty:

- **Primary regions:** Hosted in MODCloud iACE (Azure PaaS), with access from MODNet/MML via the Boundary Protection Service (BPS).

12.5 Data Transfer:

Data does not move outside approved regions other than as documented in the sub processor list and the DPA.

12.6 Audit and Logging

Scope: authentication events, admin actions, configuration changes, data imports/exports, approvals/decisions, and key user actions; time is NTP-synchronised

12.7 Retention:

Buyer access: selected audit is viewable in product; full audit export available on request (see Section 7.0 Offboarding and Exit).

12.8 Backups and Disaster Recovery

- **Integrated backups:** databases and core datasets backed up on a scheduled basis (full every 24 hours) restores have been used successfully between instances.
- **DR testing:** conducted to a documented cadence; last successful test date available on request.
- **Restore process:** initiated on ticket by named buyer admins, scheduled in UK business hours.

12.9 Assurance

- **Programme artefacts:** PRIISM iACE deployment tracked through DD Technical Release Readiness Assessment (TRRA) ; iACE production installation and ITHC completion recorded in the TRRA history.
- **Supplier endpoints:** RII management devices operate under corporate controls including CE+ posture.

12.10 Vulnerability Management

- **Baselines and scanning:** DISA STIG/SRG baselines applied where applicable; ACAS used for compliance checks.
- **Penetration testing:** Independent testing performed in line with accreditation activities (ITHC)

12.11 Sub-Processors

The service uses approved sub-processors for hosting and operational functions; each is bound under the DPA and, if applicable, international transfer safeguards.

DPA annex to include, per entity: legal name, function, processing region(s), data categories, and transfer mechanism if outside UK/EEA.

12.12 Incident Reporting and Breach Response

- **Detection and escalation:** platform health and security alerts are monitored; run-books define escalation paths.
- **Buyer notification:** the supplier notifies the buyer without undue delay after confirming a personal-data breach or a materially impactful security incident, providing initial facts, scope and mitigations, with updates until closure.
- **Report contents:** summary, timeline, affected systems/data, remedial actions, and prevention steps.
- **Channels:** notifications to named buyer admins via **email**; P1 security events may additionally trigger phone contact.

12.13 High-level Architecture

- **Hosting and Stack:** PRIISM is hosted in MODCloud iACE using Microsoft Azure PaaS. It is delivered as a SaaS application composed of Spring Boot microservices, orchestrated within Kubernetes containers. The underlying data layer utilizes technologies including Hadoop/HDFS, Accumulo, Elasticsearch, Redis, and MongoDB.
- **Web Access:** Users access the application via standard HTTPS/TLS over port 443 through an external reverse proxy and gateway service, requiring client PKI certificates for authentication.
- **Security Services:** Security is enforced through PKI client certificate authentication, combined with policy, role, and rule-based authorization controls, plus mandatory access control enforced at the storage layer. Security baselines (e.g DISA STIGs/SRGs) and vulnerability scans are incorporated into the build and pre-deployment process.
- **Data Ingest:** Apache NiFi pipelines are used to handle data streams, including PAI and ADS, with analytics microservices providing data enrichment.
- **Environments:** Separate development, pre-production, and production environments are maintained, with access strictly controlled via standard HTTPS endpoints.

12.14 Tenancy and Isolation Model

- **Model**: Logically segregated single-tenant instance per buyer within shared infrastructure, i.e., MODCloud iACE
- **Isolation Controls:** Access controls (Role-Based, Policy-Based, Rule-Based) and Mandatory Access Control at the storage level ensure tenant data separation within the shared platform infrastructure. Network level isolation is provided by the underlying Azure environment. Support for IP allow-listing can be configured upon request.

12.15 APIs and Integration

- **API Surface:** The service exposes RESTful APIs documented using the OpenAPI specification via the PRIISM Core API and gateway. An optional GraphQL "super-graph" interface is available for ontology queries and subscriptions.
- **Authentication Model for APIs:** APIs require the same PKI client-certificate / mutual TLS authentication and are subject to the same policy and role-based authorisation checks as the UI. Endpoints are not directly exposed beyond the reverse proxy/gateway.

- **Data Formats and Standards:** The service supports relevant standards, including USMTF and ASCA for targeting workflows, and Open Geospatial Consortium (OGC) / NATO Vector Graphics (NVG) for geospatial outputs, where applicable.
- **Connectors/Sources:** Data ingestion via Apache NiFi supports PAI feeds and integration with MOD authoritative sources.

12.16 Performance and Scale

- **Proven Loads:** The PRIISM platform has demonstrated scalability, supporting deployments with 18,000+ users in allied command and control programmes. The PRIISM-JTP module has sustained 600+ target entries over a continuous 6-week period and demonstrated throughputs of 250 targets per day in exercises.
- **Architecture:** The architecture is designed for horizontal scalability using Kubernetes for container orchestration, distributed search/indexing (Elasticsearch), and caching (Redis).
- **Latency and Concurrency:** The PRIISM platform is based on a scalable set of services that can be resourced to support active concurrency up to 200 users and beyond. PRIISM generally is validated to ensure a latency of 200 ms for standard data operations. Latency metrics can vary based on client network latency to the SaaS instance. Advanced features using Gen AI and LLMs may induce a longer latency based on LLM latency profiles.

12.17 Dependencies and Connectivity

- **Buyer-Side Prerequisites:**
  - Buyer manages client certificate issuance and lifecycle via their identity processes.
  - Users require browser access to the service's HTTPS endpoint(s) on port 443. DNS is typically under an iace.mod.gov.uk subdomain.
  - Buyer is responsible for any required IP allow listing or VPN configuration on their network.
- **Required Ports:** Standard HTTPS (port 443) outbound from the buyer network to the service endpoint.

12.18 Roadmap (Non-Binding)

Near term development is driven by MOD exercises and assurance activities (e.g JSP 453). Potential areas include integrations with additional effectors and allied systems, UI refinements for targeting workflows, and ongoing iACE accreditation tasks. This roadmap is indicative and subject to change based on buyer direction and priorities.

13.0 After Sales and Account Management

Contact: Please see section 16

RII provides ongoing account management to ensure the service meets operational needs. To address specific operational gaps, the following services are available and mapped to the Pricing Document:

- **Managed Operations & Support:** Comprehensive supplier-managed operations, including system administration, patching, and Service Level Agreements (SLAs), are captured under Sustainment (Pricing Items L2-10 through L2-12).

- **Enhanced Training:** Comprehensive, hands-on operational training and bespoke scenario development are captured under Integration and Support (Pricing Item L2-17).
- **Custom Reporting:** The development of bespoke reporting packs or dashboards to meet specific command requirements is captured under Consultancy & Support (Pricing Item L2-18) for labour-intensive requirements, or Ancillary Services (Pricing Item L2-19) for specific data connectors.
- **Surge Support:** General staff augmentation and technical assistance are captured under Consultancy & Support (Pricing Item L2-18).

14.0 Social Value

RII delivers social value through actions that are measurable and repeatable across all public sector buyers. The G-Cloud 15 framework identifies four Social Value missions relevant to this agreement.

Mission 1: Kickstart economic growth

1. **Skilled jobs and sovereign capability:** We maintain a UK presence and invest in skills and capability development aligned to defence digital priorities, including secure software engineering, operations, and cloud-native delivery.
2. **Support to the land industrial base:** We support the Land Industrial Strategy (LIS) outcomes by contributing to a skilled workforce, investing in research and development, and designing for sustained, sovereign exploitation through documentation, knowledge transfer, and open interfaces.
3. **Transparent and ethical supply chain practice:** We apply due diligence and contractual controls designed to prevent modern slavery and human trafficking in our supply chain and subcontracting, including a code of ethics, partner vetting, reporting routes, and contract clause flow-down where applicable.

Mission 2: Make Britain a clean energy superpower

1. **Carbon reduction commitments and reporting:** We measure and manage our carbon footprint and commit to a quantified reduction plan, including annual reporting on emissions and environmental performance metrics in accordance with PPN 006. Our most recent report shows a 4% emissions decrease since the base year, with RII currently 1% ahead of its target for NetZero carbon emissions by 2050.
2. **Lower-carbon delivery by default:** We prioritise virtual-first delivery to reduce travel and associated emissions, with travel minimised and managed where visits are essential.
3. **Sustainable technology practices:** We apply sustainable hardware lifecycle practices (repair, reuse, responsible disposal) and promote resource-efficient engineering practices, including optimising workloads and deployments for efficiency.

Mission 3: Break down barriers to opportunity

1. **Apprenticeships, training, and pathways into digital roles:** We commit to widening access to digital and software engineering skills through apprenticeships and community engagement

activities, including a minimum of two apprenticeships and two community hackathons per year, tracked and reported.
2. **Targeted outreach and partnerships to increase participation:** We maintain and expand partnerships that support underrepresented groups into digital careers and provide mentoring and coaching pathways.
3. **Armed Forces community support:** We are a signatory of the Armed Forces Covenant at Bronze level and support veterans through recruitment and community participation.

Mission 4: Build a National Health Service fit for the future

This listing is a SaaS product used by public sector teams to coordinate work, improve decision traceability, and support operational reporting. The same Social Value commitments above apply to National Health Service buyers and delivery teams, particularly:

1. Digital skills development and workforce pathways that increase local capability and reduce dependency on scarce specialist talent.
2. Lower-carbon delivery practices through virtual-first operating norms, reducing travel emissions associated with support and collaboration.
3. Ethical and responsible business conduct in supply chain management, supporting safe and compliant public sector procurement.

Measurement and reporting
On request, RII will provide an annual Social Value report summarising performance against the commitments described above, including participation metrics and progress against environmental targets.

15.0 Termination Process

The Framework Agreement or a Call-Off Contract may be terminated for convenience with 30 days written notice to RII from CCS or Buyer, respectively. However, termination for cause may be implemented immediately. Also, RII may terminate a Call-Off Contract if the Buyer fails to pay an undisputed invoiced sum (worth over 10% of the annual Contract Value) within 30 days of a Reminder Notice.

If the Framework Agreement or a Call-Off Contract are terminated, whether for convenience or cause, RII will take the following steps in accordance with the PRIISM Exit Management Plan and Contract Schedules and Terms to ensure an orderly shutdown and seamless transition, as applicable:

1. RII will set up regular transition meetings with the Buyer to ensure coordinated and orderly shutdown and transition activity.
2. Communications regarding the termination will be coordinated between the Buyer and RII, particularly to the User and Assurance communities, as well as to any connected or dependent services.
3. RII will establish an Exit Management Risk Register by which RII and Buyer will identify potential risks during the transition period and establish specific controls to implement for mitigation.

4. RII understands that the Buyer may issue a Termination Assistance Notice, by which RII may be required to provide assistance for up to 12 months after the end date of the contract, during which it will continue to provide deliverables and services.
5. All Buyer data and assets will be returned or deleted, as directed by Buyer. For any data securely erased, RII will provide a certification when complete.
6. All connections to Buyer networks, APIs, and external data feeds will be removed. Any commercial hosting arrangements dedicated to the Buyer deployment will be terminated or repurposed. Third-party software licences linked to the Buyer implementation will be cancelled.
7. Data Scope and Extraction
    a. **Identification of Data Sets:** Prior to the exit date, RII and Buyer will finalize the "Data Migration Scope" as part of the transition meetings. This includes all user-generated content, system logs required for audit, and metadata.
    b. **Standardized Formats:** Data will be extracted into non-proprietary, machine-readable formats (e.g., CSV for structured data, PDF or JSON for documents/metadata) to prevent vendor lock-in.
    c. **Transfer Mechanism:** To ensure security compliance, data will be transferred via a secure, encrypted method agreed upon by the Buyer accrediting authority (e.g., a dedicated SFTP or an encrypted physical drive).
8. Should RII be performing services on Buyer premises, RII will vacate the premises, remove its equipment, and leave the site in a clean and safe condition.
9. RII will cooperate with the handover and re-procurement (if applicable) of services. If the termination is for cause, re-procurement support may be at no cost to the Buyer.
10. RII will provide a final invoice that includes all remaining monies owed, to include costs incurred for reasonable committed and unavoidable losses. In the event of a termination for cause, RII will repay any charges paid in advance for services not yet delivered.

16.0 Contact Details

Research Innovations Authorised Representative:
Michelle Adams
Vice President, Contracts and Supply Chain
+1 571 294 8233
GCloudTeam@researchinnovations-uk.com

17.0 Glossary

Core Systems & Platforms
PRIISM™: A secure, supplier-hosted Software as a Service (SaaS) environment for military planning, coordination, and situational awareness.

PRIISM Decision Advantage: A unified digital workspace for military planning and coordination.

PRIISM Joint Targeting Platform (PRIISM JTP™): A module that supports the entire targeting cycle, including development, validation, and assessment.

PRIISM Information Advantage Platform (PRIISM-IA): A web-based mission support product for Information Operations (Info Ops).

PRIISM Integrated Network (PRIISM-IN): A SaaS solution for Network Operations (NetOps) and Command and Control (C2).

MODCloud iACE: The Ministry of Defence infrastructure where the PRIISM service is primary hosted.

Technical & Architectural Terms
API (Application Programming Interface): Tools and protocols for building and integrating software applications.

Data Fabric: A Federated architecture that ingests data from disparate sensors and systems to create a unified view.

LLM (Large Language Model): A Generative AI capability used to process complex text and data for planning and decision-making.

MOSA (Modular Open Systems Approach): A method to ensure interoperability and eliminate vendor lock-in.

RBAC (Role-Based Access Control): Permission management ensuring users only access data appropriate to their role and clearance.

SSO (Single Sign-On): A session and user authentication service that permits a user to use one set of login credentials to access multiple applications.

Operational & Military Terms
C2 (Command and Control): The exercise of authority and direction by a properly designated commander over assigned and attached forces.

COA (Course of Action): A possible plan that may be followed to achieve a specific mission.

COP (Common Operating Picture): A single display of relevant information shared by more than one command.

IPE (Intelligence Preparation of the Environment): A systematic process of analyzing and visualizing the environment in a specific geographic area.

NetOps (Network Operations): The activities performed by network administrators and operators to maintain and manage a network.

Target List Management (TLM): The process of managing and prioritizing target lists for military operations.

Security & Compliance
DPA (Data Processing Agreement): A contract governing the processing of personal data, aligned to UK GDPR.

IAtO (Interim Authority to Operate): A temporary authorization to operate an information system.

OFFICIAL-SENSITIVE: A classification for data that requires additional protection due to its sensitive nature.

PKI (Public Key Infrastructure): A framework for managing digital keys and certificates to ensure secure communication.

TRRA (Technical Risk & Remediation Assessment): An MOD assurance process used to track deployment risks.