**Formal Risk Assessment and Operational Justification for Granting Scoped Central Administration Access to the IPDS Development Team**

**1. Operational and Technical Tasks Requiring Farm-Level Administrative Access**

The RFQ ("B08 - RFQ Attachment (PWS)") clearly outlines several tasks that *cannot be executed effectively without SharePoint Central Administration (farm-level) access*. These include:

**a. Timer Job Configuration**

* The IPDS application involves **routing workflows**, metadata reminders, and automated document dissemination, which rely on timer jobs for task execution and notifications.
* These require visibility and control over timer job definitions, history, and execution—all accessible only via Central Admin or equivalent PowerShell management interfaces.

**b. Diagnostic Tooling**

* The platform must enable diagnostics for performance issues, integration failures (e.g., with SIPP, Publications Warehouse), and task execution delays.
* ULS logs alone are insufficient for root cause analysis involving service proxies or config DB inconsistencies, as confirmed in Microsoft documentation and reiterated in the Rebuttal documents.

**c. Service Application Maintenance**

* The system requires integration with:
  + DOI Azure Active Directory (for authentication and metadata population),
  + Web services/APIs for SIPP and ScienceBase.
* Managing these integrations involves configuring **User Profile Service**, **Search Service**, and secure **Service Application Proxy Groups**, which require farm-level access.

**d. Platform-Level Monitoring**

* Per the PWS, IPDS must support:
  + Uptime requirements,
  + Data integrity monitoring,
  + Automated clean-up jobs,
  + Performance tracking across 3,000 users and 160,000 records.
* Monitoring tools like **Health Analyzer**, **Diagnostic Logging Configuration**, and **Resource Throttling** settings are all administered via Central Admin.

**2. Policy Justification for Scoped Administrative Access**

**a. NIST SP 800-53**

* **AC-6 (Least Privilege)**: Supports *role-based administrative scoping* with minimum required access.
* **AC-5 (Separation of Duties)**: Allows role blending when:

“Risk is low and compensating controls (e.g., logging, reviews) are in place”.

**b. OMB Circular A-130**

* **Section 8(b)(4)(ii)** mandates agencies to:

“Ensure information systems maintain availability through appropriate technical controls…”

* Limiting farm access required **violates system availability and continuity mandates**.

**c. USGS IT Security Program Plan v5.0**

* **Section 4.3.2**: Emphasizes that access controls must:

“Enable personnel to fulfill mission-essential functions and must not introduce operational barriers.”

* **Section 6.2**: Requires access to:

“Monitoring tools and logs across all operational layers.”

**d. USGS Manual Chapter 600.5**

* **Section 7** allows:

“Assignment of multiple roles... in small teams... if periodic audits and reviews are enforced.”

**3. Rebuttals to Common Objections**

**a. Violation of Least Privilege**

* Misunderstanding: Least privilege means *granting minimum access* **required**, not *denying* necessary access.
* Scoped access via Central Admin with JEA and audit controls directly fulfills the least privilege policies.

**b. Violation of Separation of Duties**

* Contextual application is supported:
  + USGS and NIST permit SoD flexibility in low-risk, small teams.
  + Logging, peer review, and change management are **valid compensating controls**.

**c. Change Control Conflicts**

* Developers executing changes ≠ owning governance.
* ITSM-01 policy:

“Bureau teams are responsible for executing approved changes… under CAB processes”.

* This model is already standard across USGS.

**d. ULS Logs Are Sufficient**

* Technically inaccurate. ULS:
  + Lacks visibility into farm-level issues (e.g., misconfigured service proxies).
  + Cannot substitute Central Admin views like Health Analyzer and timer job status.

**e. IPDS Should Build Its Own Farm**

* Violates:
  + DOI IT Shared Services Framework
  + USGS OCIO guidance
  + OMB A-11 and FITARA
* would increase cost, delay delivery, and reduce alignment with enterprise security baselines.

**4. Risk Implications of Denial**

|  |  |
| --- | --- |
| **Risk Area** | **Implication** |
| **Project Timeline** | **July 14, 2026,** the modernization deadline will be missed due to dependency on external admin teams for every config, diagnostic, or deployment task. |
| **Operational Continuity** | Lack of direct control will lead to delays in issue diagnosis and system downtime — undermining user trust and continuity. |
| **Policy Compliance** | Inability to maintain audit trails, Health Analyzer thresholds, or integrate properly with USGS systems will break FSP and OMB mandates. |
| **Cost & Duplication** | Without access, separate infrastructure may be proposed — violating DOI shared services and inflating costs. |

**5. Recommended Compensating Controls**

To balance access and governance:

1. **PowerShell Just Enough Administration (JEA)**
   * Restrict cmdlets to timer job, service proxy, and diagnostic functions.
2. **Scoped AD Role Assignment**
   * Access tied to specific IPDS-related service applications or site collections.
3. **Quarterly Access Review**
   * Documented in Change Management Plan; reviewed by IT Security Office.
4. **Formal Change Management**
   * All configuration changes are routed through CAB for approval.
5. **Audit Logging & Alerting**
   * Enable centralized audit of all privileged operations.
6. **Access Expiry & Revalidation**
   * Time-bound access with justification renewal requirements.

**6. Conclusion and Recommendation**

**Recommendation**:  
Authorize **scoped SharePoint Central Administration access** for the IPDS development team. Limit access to specific operational components and implement robust compensating controls.

**Rationale**:

* **Technically Necessary**: Required for timer jobs, service apps, diagnostics, and integrations.
* **Policy Supported**: Aligned with NIST SP 800-53, OMB A-130, and USGS IT Security Plan v5.0.
* **Operationally Efficient**: Prevents avoidable delays and dependence on admin bottlenecks.
* **Governance Ready**: Risk can be mitigated using standard enterprise access control mechanisms.

Denial of this access would hinder modernization, violate multiple policy mandates, and jeopardize project success.