**Subject:** Rebuttal to Concerns Regarding IPDS Team Access to SharePoint Central Administration

**Summary of Concerns and Rebuttals**

**1. Concern: Central Administration Access May Impact Other Sites**

**Rebuttal:**  
Access to Central Administration does not have to be global or unrestricted. The SharePoint platform supports **delegated administration** and **role-based access control**. Scoped access can be granted solely for IPDS-related components (e.g., specific service applications, timer jobs, or site collections). This model is consistent with **USGS IT security policies** and **NIST SP 800-53 AC-6**, which supports least privilege with defined roles.

Moreover, collaboration bottlenecks between development and admin teams hinder agile response and maintenance. Federal mandates such as **OMB Circular A-130** and the **Federal CIO Council's Shared Services Strategy** promote efficient inter-team cooperation and timely system upkeep.

**2. Concern: Violates Separation of Duties (SoD)**

**Rebuttal:**  
While SoD is an important principle, **NIST SP 800-53 Rev. 5 (AC-5, AC-6)** explicitly allows for blended roles when risk is low and compensating controls (e.g., audit logging, approvals, and periodic reviews) are in place. Within the USGS environment, similar models are already in practice for other applications.

In this case, the access required by the IPDS team can be limited to **non-administrative or scoped administrative tasks**, with oversight through change control processes and logging mechanisms, preserving the integrity of SoD principles without restricting operational efficiency.

**3. Concern: Admins Responsible for Change Control, Patching, and Deployment**

**Rebuttal:**  
This responsibility is not in conflict with scoped access. Allowing the IPDS team to conduct targeted application-level configurations (such as timer job scheduling or debugging service application settings) does **not circumvent or replace formal change control**.

Access can be granted with documentation and limited by scheduled change windows, fully in line with **USGS ITSM protocols** and existing CAB processes. This enhances responsiveness without undermining system governance.

**4. Concern: Security Risk – Violates Least Privilege**

**Rebuttal:**  
The **principle of least privilege** does not equate to denying necessary access; it mandates **only granting access required to perform authorized duties**. As outlined in **USGS Information Security Handbook** and **NIST SP 800-53 AC-17**, this can be achieved with:

* Scoped roles (e.g., site collection or service app admin)
* Access justification and approval workflows
* Periodic access reviews and full audit logging

Furthermore, tools like **PowerShell Just Enough Administration (JEA)** and SharePoint’s Central Admin delegation features allow fine-tuned access control, minimizing exposure to unrelated systems.

**5. Concern: ULS Logs Are Sufficient for Troubleshooting**

**Rebuttal:**  
ULS logs offer limited insight, mostly restricted to application-layer issues. They do not capture deeper system-level events such as:

* Timer job execution failures
* Configuration database inconsistencies
* Service proxy registration issues
* Health analyzer rule violations

Access to certain Central Admin components, such as diagnostic logging configuration or the Health Analyzer dashboard, is often required to resolve issues efficiently. Denying this access leads to dependency delays and violates best practices promoted under **OMB’s Modernization and Shared Services guidance**.

**6. Concern: IPDS Should Build a Separate SharePoint Farm**

**Rebuttal:**  
Creating a separate farm introduces **unnecessary infrastructure duplication**, which contradicts:

* **OMB Circular A-11**: requiring efficient use of IT resources
* **FITARA**: encouraging shared services and centralized management
* **USGS infrastructure rationalization goals**

Moreover, separate environments dilute testing fidelity, increase maintenance overhead, and reduce alignment with enterprise security baselines. Controlled access within the existing environment provides better governance, continuity, and operational alignment.

**Conclusion**

The IPDS team’s request for scoped Central Administration access is operationally justified, risk-manageable, and compliant with federal and USGS IT governance frameworks. Denying access based on legacy control models introduces inefficiencies and delays inconsistent with modern federal IT mandates.

With appropriate controls — including scoped access, audit logging, and formal change management — this access enhances agility and service responsiveness while preserving system integrity and compliance.

**Recommendations:**

* Approve scoped Central Admin access for the IPDS team, limited to required components only.
* Enforce access controls via AD roles, JEA, and SharePoint delegation features.
* Conduct quarterly access reviews and tie access to formal change management workflows.
* Avoid infrastructure duplication unless mission-critical separation is required.

Please advise if further clarification, risk analysis, or policy citation is needed to support this recommendation.