- **What services should the public cloud deployment offer to the customers?**
    - Structural *private* network connectivity to on-prem edu campus network
        - This traffic should be segmented for two use cases:
            - Central IT data center extension
            - Cloud connectivity for individual colleges and research groups
    - DC extension into cloud for central IT
        - Domain controllers
        - DNS (eventually)
        - Storage
        - Disaster recovery for some applications and storage
        - LMS
- **How will the users consume those services? Will they use Internet access or will you have to provide a more dedicated connectivity solution?**
    - Per requirements by leadership, users must leverage a structured private connection between campus and cloud. No external connectivity for now.
- **Identify the data needed by the solution you're deploying. What data is shared with other applications? Where will the data reside?**
    - Financial records, student records, employee records, NMS data, etc.
    - This data currently resides in multiple SAN environments and will need to be replicated into cloud storage environments
- **What are the security requirements of your application?**
    - User-facing nodes and applications must be secured by a border firewall along with host-based firewall in some cases
    - Security policy implementation must be as familiar as possible to today's tooling
- **What are the high availability requirements?**
    - Initially, we are looking to use our on-prem load balancer to distribute workloads between on-prem and cloud hosts. Alternatively, we may pursue a DR mechanism where services are enabled in the cloud by manual intervention if on-prem were to fail or undergo a major maintenance.
- **Do you have to provide connectivity to your on-premises data center? If so, how will you implement it?**
    - We are I2 members and will be using their "cloud connect" service. Initially, they will hand us a VLAN which we will extend behind our data center border firewall so our information security team can apply policy in a familiar way. This VLAN will extend through I2 and will terminate on an expressroute connection. Eventually, we would like to replace the VLAN with an L3VPN (provided by I2) for more flexibility, but we are currently limited by knowledge gaps on how to apply border security policy at the cloud edge
- **Do you have to implement connectivity to other (customer) sites? If so, how will you implement it?**
    - Building off of the last point, we may have to use multiple VLAN extensions from cloud services to on-prem colleges and researchers. I don't love using VLAN segmentation for security policy, but right now the cloud edge security knowledge gap is a hugely limiting factor. Once we

overcome this I would like to use a single L3VPN and apply border policy at the cloud edge.