The REN-ISAC Technical Advisory Group would like to call attention to Apple's new iCloud Private Relay, which, if used, may impact your network visibility and IT security.

Here are some key points about iCloud Private Relay:

- Apple iCloud Private Relay allows applications on macOS or iOS devices to potentially bypass local network monitoring and the protection that monitoring provides.
    - Web traffic, DNS queries, and potentially other traffic are tunneled via QUIC over port 443 with TLS 1.3. This traffic will typically be opaque to network monitoring.

Client   Access network   Ingress Proxy   Egress Proxy   Server

- Users may be unaware that they're using Private Relay.
    - The service requires a paid iCloud+ account, which many Apple users may already have.

- The feature was recently released in the latest macOS and iOS major version updates as a Public Beta.

Private Relay can be disabled for your network. If you have control over your local DNS, you can force specific domain names to return a negative response for
- mask.icloud.com
- mask-h2.icloud.com

Client   Access network   Ingress Proxy
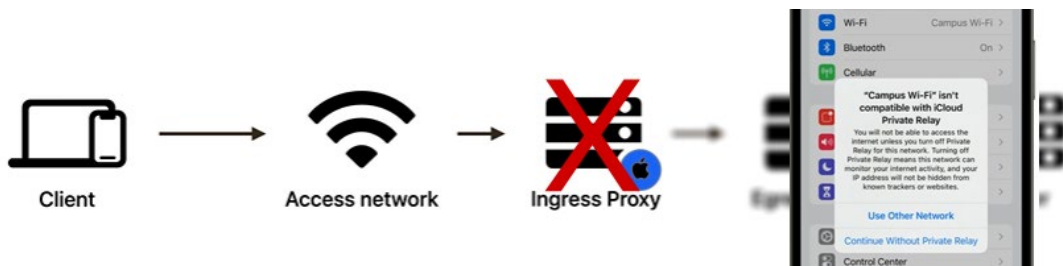
Blocking access to Private Relay may be reflected as a message on an Apple device, leading users to
- inquire about your decision to block it
- potentially seek details about your institution's network traffic monitoring program

We recommend institutions work with their network and security staff to understand how
- Domain name resolution is conducted at their institution
- DNS choices by users can impact user privacy and security
- IT security operations and protections may be impacted
- User support may be impacted
- Reliability, availability, and performance may be impacted

To prepare, we recommend that you
- Review documentation on [iCloud Private Relay](#)
- Review the [REN-ISAC advisory on DNS over HTTPS (DoH)](#)
  - DoH has similar issues as iCloud Private Relay
- Determine whether you want to allow or disallow use of iCloud Private Relay at your institution

In addition to the documentation provided by Apple, an [article published by Macworld](#) provides greater detail about the service.