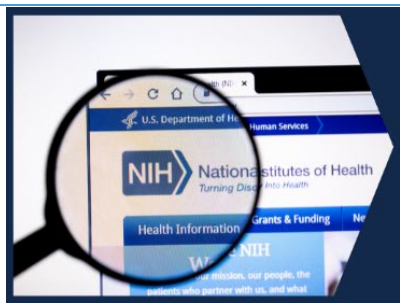

New NIH Requirements for Identity Assurance

The National Institute of Health (NIH) is increasing security for their systems. The University met the first of their requirements last September, when the NIH began requiring multi-factor authentication for those logging in to their systems. For the next phase, the NIH will require identity assurance, which means stronger proof that a person is who they say they are.

The NIH uses the criteria defined in the REFEDS Assurance Framework to define levels of assurance. REFEDS, which stands for "Research and Education FEDerations," is an organization that represents the requirements of research and education related to access and identity management.

REFEDS defines four levels of identity proofing assurance: low, medium, high, and "enterprise equivalency." Each level answers the question, "How well does your identity proofing process let you be sure that the person is actually who they claim to be?"

June 30: Local Enterprise Equivalency

By June 30 we need to be able to assert "local enterprise equivalency." What this means is that when a person logs on to the NIH systems, our system passes an attribute that says that they are trusted to access our internal administrative systems. This level of assurance relies on the assumption that if the person is trusted to access the University's administrative systems, they can be trusted to access some external resources as well. By administrative systems, REFEDS means systems that deal with:

- money (for example, travel expense management systems or invoice circulation systems)
- employment-related personal data (for instance, employee self-service interfaces provided by the Human Resources systems)
- student information (for instance, administrative access to the student information system)

December 31: Low, Medium, High Level of Assurance

By December 31 we need to have a system in place for specifying whether a person's level of identity assurance is low, medium or high as defined by REFEDS. These rankings are related to NIST 800-63, which comes from the federal government. Often providing this assurance requires evidence such as in person verification of government documents and a written procedure.

If we aren't able to achieve all three levels, we need to demonstrate that we have a plan for how to get there. Considering the complexity of achieving the high level of assurance, our goal is to assert low assurance for all UNC users, identify who needs medium or high assurance, and develop a process to provide the high level of identity assurance.

Who this affects

Researchers, grant awardees, principal investigators (PIs), and any other faculty or staff member who needs to log in to the NIH systems using UNC credentials.

Next Steps

- A project team is being formed to include representatives from all relevant groups in ITS and campus units, including the Office of Sponsored Research, the One Card Office, the PID Office, the Information Security Office, the Identity Management team, and the ITS Service Desk.
- To identify the gaps that need to be addressed, the project team will map the University's current processes related to identity assurance, such as the I9 process and the photo ID process, to the criteria defined in the REFEDS Assurance Framework.

Resources

- InCommon: Updates on NIH Identity Requirements and Plans
- Confluence: Get NIH Ready (video)
- NIH: Security Requirements FAQ