Good Morning,

I'm reading through the NST SP 800-181 draft document that was sent out this morning, and have to compliment your team on the incredible work that has been done. This is moving in a direction that personally I feel is something that has been needed for a long time.

In A.3 NICE Framework Work Roles, I'm wondering if there is too much lumped into OM-ADM-001 System Administrator Work Role. This is following a traditional view of the System Administrator where everything is put into a catch all role. I have been the co-lead for the Forest Service/USDA Privileged Access Management (PAM) project for the last year, studying how user accounts have been put together.

In most organizations the User Account Management roles have traditionally been under what you have the as the System Administrator. Perhaps this needs to be broken out into its own role that is based on ICAM methodologies. The new role would be User Account Administrator, or perhaps ICAM Manager. This really needs to be broken out into a new Work role for a couple of reasons. One, having it under the System Administrator can potentially cause a conflict in regards of Separation of Duties. Second, User Account management requires a little bit of a different view of the IT environment, there needs to be an understanding of the relationship between Business Roles, IT Roles, and the entitlements that a user is granted. As a whole we really need to move away from the traditional user account management practices being done by a Systems Administrator and move towards automated systems that are driven by workflows and system intelligence. This role needs to be in addition to the System Administrator (ADM).

The same case could be made for creating a Data Protection Administrator or Storage Systems Administrator (overseeing, and conducting backup and recovery tasks). This is a specialist work role that is also lumped into the Systems Administrator. As a former SAN manager, this is a highly specialized area that should be separate from the traditional Systems Administrator (ADM). Protecting Data from includes not just the traditional SAN but includes replication, snapshots and backups.

Thank you for sending this out and asking for feedback. It is great work, and I'm really glad to see it is something being worked on. Please reach out to me if you have questions.

Dan Hawkins
IT Security Analyst/IT Fellows
USDA Forest Service
Cyber Security Office

3833 S. Development Ave
Boise, ID 83705
www.fs.fed.us

Caring for the land and serving people