Feedback to NIST SP 800-171Rev2
Mauricio Tavares [redacted]

Chapter 2

1. 2.1. (p.5) I may be nitpicking here, but the italics in "federal information designated as CUI has the same intrinsic *value* and potential *adverse impact* if compromised"? The use of Italics here on "value" and "adverse impact" seem to imply that CUI has the same
   - intrinsic value
   - potential adverse impact

if compromised. CUI's value (hopefully) is not dependent on whether it is compromised or not. IMHO, the blue rectangle on the top of p.6 explains that better.

Chapter 3

1. 3.1. (p.10) Access Control: Basic Security Requirements should include a temporal cause.

Ex:

1. Limit system access to the types of transactions and functions that authorized users are permitted to execute (3.1.2) for the period of time said access is required, not before or after. I understand the discussion for 3.1.2 specifically mentions restrictions on time-of-day, day-of-week, and point-of-origin access, but the point I am making here is that access always have a lifetime.
2. 3.1.5 (p.12) I would add something like "limited privileged accounts are roles that can perform limited privileged functions on specific systems such as starting a backup operation: limited privilege user can start the backup but may not edit the parameters." after the first sentence of the second paragraph under Discussion.
3. 3.1.13 (p.14) Cryptographic mechanisms are not enough to provide confidentiality of remote sessions. There are other kinds of remote sessions besides VPN (3.1.12); encrypted VNC comes to mind. I know I used "encrypted," but that only covers one aspect of protecting confidentiality; the other is considering how the application isolates itself from the rest of the computer being used to remote access the resource.
4. 3.2.1 (p.16) Pet peeve of mine is "making someone 'aware' of security risks." Making aware is not enough for it does not imply understanding or having a real relationship with it. Case in point is saying to a manager "weak passwords are bad and MFA good" (awareness) vs "Multifactor authentication can save $X to the company" (relating security risk to a tangible outcome manager can relate with). Ok, this is me venting, but there it is.
5. 3.3.5 (p.19) Replace "rather collectively" with "rather collectively creating a more complete view of events."
6. 3.3.8 (p.20) Add something like "Access to auditing tools allow malicious users to probe systems for restricted information and vulnerabilities."
7. 3.3.9 (p.20) is making a case for the limited privilege user I mentioned earlier. So, if that change is incorporated, we can then refer to 3.1.5.
8. 3.4.8 (p.23) The processes being talked here are allow by default vs deny by default. It may be better to be more explicit, say "The process used to identify software programs that are authorized to execute on systems, and deny everything else by default, is commonly referred to as whitelisting."
9. 3.4.9 (p.23) Add somewhere "some software can be run with unprivileged user rights from the user account."
10. 3.5.3 (p.24) Note most MFA require network access to the, well, MFA server; when a system is not able to connect to the network, local privilege access requiring MFA will end badly. Ask me how I know. Bottom line: MFA where feasible, but it is not a panacea.
11.