Greetings,

I wanted to offer seven key ideologies for the framework from 20 years of working in the DoD on classified networks.

1) The formerly disjointed systems are increasingly becoming integrated as equipment is recapitalized under new guidance and regionalization efforts. This increases the attack surface of these components, so the obvious question must be asked; would it be cheaper to leave the disconnected systems (SCADA, etc) offline, instead of bringing them into the global community where we're forced to protect them?

2) IT regionalization efforts empower government entities, not because they are good at the task, but because they have been chosen. This is the opposite of the X-Prize system in the commercial sector, where a $10 million "prize" is offered to a team that brings forth a solution to a problem. The best solution always wins. Unfortunately, in government, we give $100 million to office X of the heirarchy and tell them to make it happen. When they fail, we just give them more money. This strategy continues to happen within the federal, state, and local government. Offices are given a task not because they are suited for it, but because they are in the right place, at the right time.

3) IT regionalization, especially within the government and DoD, tends to enforce compliance at all costs, with a one-size-fits-all approach. This damages the role of government offices' actual mission/purpose, the further down in the heirarchy we get, where the government interacts most often with the taxpayer. In many cases, especially the DoD, the mission gets lost in the hustle, and compliance with the rules becomes the mission. All exclusions become burdensome documentation to the internal government customers whose job it is to use the computing tool before them, to do their job.

4) Despite the fact the SP800-53 and others declare those guidelines off limits for national security systems (45 USC, Section 3542 I believe), many DoD entities still reference and enforce them. Why doesn't NIST believe SP800-53 should be applied to these systems?

5) There are too many government rules out there governing what we do on computers. There is no single-source document, or even a single location where they can all be sourced. Furthermore, as soon as the feds write the rules, they're out-dated.

6) Cyber requires talent. It requires white-listing, the latest patches, compliance by users, and accountability by those in charge. What fails to get delivered (repeatedly) is process. ITIL, MOF, you name it. Many government entities fail to secure their IT properly because they're not process-centric. The inspectors love process.

7) Final thought on DoD Instruction 8570. This is the driver that forced CompTIA to make their certs renewable. They wanted all Information Assurance certifications to comply with ANSI/ISO/IEC 17024 standards, (aka continuing education requirements). Interestingly enough, this is a scenario where the government is mandating its workers meet this certification

requirement, and then forcing itself to pay for the creation of continuing education credits so its workers can satisfy those requirements, all-the-while paying a corporate entity to slap a sticker on its employs saying "yep - they're certified". I point out the failed logic so that NIST can watch out for scenarios where it may repeat.

If you have any questions, or would like to discuss anything further, I would be happy to offer more thoughts on anything. I recognize, many of my comments stray from the detailed specifics of a common NIST guide on technical implementation of securing a computer, but strategy and process are more complex and more important than the technology. I must say I haven't had a chance to read much of NIST's documentation, but my military unit is telling me we'll be going that route largely in part due to ICD503. Perhaps I just need to read more of what you have posted.

Respectfully,
Josh Melton, GG-11, US Air Force
(Retired TSgt as well)
WPAFB, OH