Name	Line No.	Comments
Reggie Williams	133	Change “CA” to CoA. CA refer to Certification Authority
Reggie Williams	131-134	Add the word “technology” after the word “process,”
Reggie Williams	144	Add “Scalability” as the fourth bullet item
Reggie Williams	155	Add “Scalability”; Scalability ensures that product, processes, technology or services capability of being modified or changed based upon other compliance conformity assessment types.
Reggie Williams	167	Add a new core area: Data Transference Evaluation: Data transference related to sending or transferring sensitive data to a supplier, third party, vendor, or a hosted provider. Ensure that controls and security / risk assessments are conducted by the data owner of the specific data to evaluate controls based upon formal contracts or statements of work.
Reggie Williams	193	Add to establish a “Governance, Risk & Compliance structure”
Reggie Williams	202	Remove terms related to cryptography. Cryptography terms should all move to 171
Reggie Williams	208	Add “technologies” after standard
Reggie Williams	218	Add. Automated activities would include a Security Operation Center (SOC) to ensure autonomous and continuing monitoring and evolution of security state of assets based upon prescribed events.
Reggie Williams	200	…..by balancing security and risk tolerances
Reggie Williams	220	This section “Supply Chain Management” should fall under 4 Some Key IT Applications. Also change to “Supplier / Vendor Chain Risk Management (SVCRM)”
Reggie Williams	222	Add the word “vendor” after supply,
Reggie Williams	256	Change to “4 Key Core Models in Cybersecurity Standardization” The term “IT Applications” would complicate the term of software application resulting in confusion
Reggie Williams	256	Question: Should Critical Infrastructure Protection (CIP) be part of Section 4?
Reggie Williams	282	Remove words related to electrical within this section. Electrical is part of 299
Reggie Williams	299	Change from “Smart Grid” to “Electrical Smart Grid”
Reggie Williams	355	Change “Cryptographic Techniques” to “Cryptographic Management”
Reggie Williams	355	Change” Identity Management” to “Identity & Access Management”
Reggie Williams	355	Change “Cyber Incident” to “Cyber Incident & Response”
Reggie Williams	369	Add: Maturity Level ”Re-Evaluation” before Reference Implementation Definition: SDO revaluates standard for changes to product/services, technical content or project.
Reggie Williams	509	Change from “Voting” to “Voting / Election Management
Coleman Wolf	General	Overall it appears to be comprehensive in breadth but lacking in depth. This may be by design, but I know I would hope to find greater detail overall.
Coleman Wolf	General	One specific issue that I did not find covered in any direct manner is the need for protection of Building Control Systems as a whole. I see “Industrial Control Systems” are covered, but these tend to be more process oriented whereas Building Control Systems include things like fire alarm systems, card reader access control, video surveillance, elevator control, lighting control, HVAC, and energy management. Building Control Systems is a subdomain with its own special considerations that also need to be addressed.
Tim McCreight	General	The realization that education/awareness training on cybersecurity resonates with my personal views. Ongoing programs could be expanded, though, to include introductory sessions within technical colleges and potentially high school students. This would link to the Enterprise Security Competency Model created by ASIS and Apollo Education Group (creating skills beyond Foundational).
Tim McCreight	General	Training programs for Government employees (regardless if they are US or other countries) should be mandatory. We continue to provide training on life safety topics (driving, worksite safety), but neglect training that could increase the resilience of an organization, or provide greater insight into the severity of an cyber incident. We rely on employees to help safeguard our information assets – creating mandatory training programs for USG and other nations would be an excellent first step.
Tim McCreight	General	Conducting assurance activities against technology is a great idea, but caution should be taken on what types of assurance or attestation are being provided. Care should be taken to ‘test’ the technology for the protection it is advertised to provide, instead of the additional ‘features’ or ‘options’ that could be invoked. Past experience has provided this commentator with enough war stories on promises made and broken from a technology perspective that even with assurances, we can only rely on technology for so much.
Tim McCreight	General	I would also encourage the development and implementation of sound, pragmatic, information security policies and procedures. While not as appealing as testing technology, foundational work like strong polices and well written standards offer some great opportunities to document actions, ensure daily activities can be audited, and provide a starting point for incident detection and resolution
Tim McCreight	General	Training and engagement with current technical staff must be a key component of this initiative. Too often current employees are left to their own devices for training and ongoing education on their chosen field. A percentage of every operating budget should have funds allocated for employees to participate in training sessions, online forums, memberships in security communities, and the opportunity to attend trade shows. This seems more of a benefit than a requirement, but in my career I have lost strong security analysts to other organizations based on their training budgets.