Section	Page	Comment
Tables	Overall	It looks like "Separation of Duties" is not covered. Given the number of high profile incidents it should be. In practice, Separation of Duties limits the blast radius and seriously affects the economics for the hacker. If you look at the major Government losses like Snowden and the OMB hack, they would have been prevented, at least significantly less impactful if SOD was incorporated. It would be good to see SOD included and elaborated on in 4.2.2.4 Identity and Access Control, tables 2, 3, 4, 5, 8, 10, 11, 14, 19, and 20.
Overall	Overall	We understand that the notion of Trust Zones, with labels of High/Medium/Low, are defined in the TIC Use Case Handbook and the TIC Reference Architecture document. And, this TIC Cloud Use Case document shows the boundaries between different Trust Zones (bridged by PEPs). (Note - we think that the term "Trust Zone" is actually misleading, and should have been "Control Zone" - but let's put that aside). What seems to be missing from this document is a mapping or description of what organizations should do *differently* in the different Trust Zones. This is a key element, which we feel is missing. Should there be *more* or *less* observation of workloads in High trust zones versus Low trust zones? What should the PEPs do when bridging from one trust zone level to another? why? The foundational concept of "zero trust" is that all networks and workloads should be treated as untrusted and potentially hostile. What differs is the amount of control that an organization can apply to different zones.
4.1 Assumptions and Constraints	4	The introduction to the document does refer to the definitions in the TIC Reference Architecture and Security Capabilities Catalog, however the new approach to network security must refer to network identity access management, as this is an essential part of Policy Enforcement Points (PEPs). Message, device, application access security is a key topic. I think it must be mentioned in Assumptions and Constraints if identity access management is excluded from the scope. Network references to VPN and UCC, as referenced, do not cover identity access security measures, e.g. DNSSEC
4.2 Conceptual Architecture	8	Table 1: Trust Zones in the Cloud Use Case for IaaS, PaaS, and SaaS - the exmple trust levels defined in this table are at odds with the current industry definitions of current level of cybersecurity threats. For example, the NIST NVD (National Vulnerability Database) also indicates that the huge number of vulnerabilities of internally deployed licensed and open source software. Hostile insiders, either paid by hackers, or just individuals with a grudge, is recognized by the major cybersecurity industry players as one of the biggest cybersecurity attack vectors in terms of both level of damage and percentage points growth. In this document, Agency Campus and Agency Service are given the highest example trust level, and the Remote User Trust Zone is declared as medium, at the same level of the Cloud Service Provider Trust Zone. These may not be good example levels - for example, large CSPs invest heavily in cybersecurity, and deliver good results. Remote user home networks are generally unmanged and unmonitored. Another example - External Entity and Web are defined as low trust. If External Entity is another Agency or a highly secure corporation which has followed the guidelines and deployed best practice Zero Trust , are they untrusted? Internet services can be very insecure or very secure, depending on the level of encryption, the identity access management deployed, the certificates, dns, application and network firewalls deployed (presuming Web here is internet services, not the network itself).
4.2	13	Before Table 1 - would be nice to define "Low, Medium and High" Trust levels. In other words - Why is Agency Campus Trust Zone is labeled as "High level Trust". Having a section explaining these definitions will help
4.2	7 to 13	I'm struggling to understand how each of the (example) trust zones got their ratings. It does feel like the decisions were driven by traditional practices like strong physical perimeters and insiders can be trusted..
1.1 Key Terms	1	A more descriptive definition of "Telemetry" would be "The process of recording and transmitting the readings (or artifacts) of a security capabilities that provide visibility into security posture."
2.OVERVIEW OF TIC USE CASES	3	Executive Order 13556, established the program for consistent handling of Controlled Unclassified Information (CUI) across the Executive Branch. Should that be referenced?
4.2 CONCEPTUAL ARCHITECTURE	7	The use of Conceptual Architecture enhances understanding.
4.2.1 Shared Security Model	9	While it is a shared responsibility model. The organization remains accountable. It would be good to reiterate that point so organizations do not think just because they contracted a CSP they are magically in compliance with the various EOs, directives, and the like.
4.2.1 Shared Security Model	9	It would be good to reiterate data must be protected while stored, processed, and transmitted. We can then go on to say this applies to all of the trust zones and while being transferred between trust zones. If we agree, I can draft some language.

Section	Page	Comment
Figure 4: Varying Levels of Responsibilities for Different Service Models	9	I like the way they represented that graphically.
4.2.2 Risk and Deployment Considerations	10	The document talks about the organization doing their Due Diligence. In reality they will be relying on Third Part Attestations like FedRAMP. It would be useful to talk through that.
4.2.1 Shared Security Model	9	Usually who is responsible for what is documented in the Risk Register and RACI diagrams. Should they be mentioned?
4.2.2.4 Identity and Access Control	11	Organizations often get into trouble with Identity and Access Control in a shared responsibility model. The Organization remains ultimately accountable for (1) being the source of truth for Identity, (2) determining the privileges based on Policy, and (3) keeping both current. This is part of the Organization's Data Governance role. The provider is responsible for implementing. This should probably be highlighted in the document.
4.2.2.6 Misconfiguration	11	This is a common problem, easily corrected. Would it help to reference some statistics like OWASP?
4.3.1 Security Pattern 1: Agency Campus to Cloud Service Provider	16	Something is wrong with the formatting of Option 1.
4.2.3.2 Service Connectivity	13	Unprotected direct connections, remote desktops, and VPNs each have their own risk. Should we talk to the concerns or is there something we can reference?
4.2	12	might want to just include Pop-Up details in the white paper instead .. almost missed it until my mouse hovered on it.
4.2.2.4	16	Should we discuss MFA in this section to mitigate mentioned security risks
4.2.2.9	17	Mentioned Cloud Security Solutions are not mutually exclusive. So a diagram showcasing similarity bet these solutions will help
5.2.1.2		Section 5.2.1.2 entitled "Email as a Core Agency Application" needs to be much earlier in the section. Following the premise security must be aligned with the mission, I would consider making this section 5.1.
5.2.1.1	60 and 61	The section as written talks to how Email can be used as part of an attack. A section needs to be added that talks to the threats to email itself using CIA as the framework.
5.2.1.2	61	Suggest changing the section title to "Email as a ***Mission Critical*** Agency Application" to more accurately describe the situation and to be consistent with other publications.
Table 19	87	Looks like protection of Data while being Processed is missing.
5.5 TELEMETRY REQUIREMENTS	91	The details of what needs to be collected, stored, shared, etc needs to be built out. Is that being handled in another document?
5.5 TELEMETRY REQUIREMENTS	91	There are a myriad of reporting and data collection requirements and more are in the works. Should this paragraph be built out to include the larger audience or is it intentionally kept to CISA?
4	4	The pattern "Secure agency campus to agency-sanctioned cloud service providers (CSPs)" should say "to and from" rather than just "to", since CSP-hosted resources may need to reach back to on-premises workloads or data
4.1	6	the assumption about BYOD traffic states "While traffic to the web from BYOD is generally out of scope for TIC 3.0...". The metadata for this traffic - especially DNS requests, should be monitored for known malicious domains, This is not difficult to do technically, and adds a lot of value. Machines accessing known malicious domains should immediately be blocked from accessing agency resources
4.3.1	20	Some formatting issue with Option 1 (at least for me) first 2 characters of each line for Option 1 is missing

Section	Page	Comment
4.4.2	39	Might be a good idea to add the definition of "Policy Enforcement Point" to the Key Terms section. What is PEP ? Policy enforcement point (PEP): This is the point where policy is enforced—that is, conditions that are subjected to policy are identified and the respective policy actions are taken
Table 4	42	For "No specific guidance" rows - Is there a reason to just have definitions ? Should these be part of Appendix C
Table 6	46	"Elastic Expansion" is actually referred to as "Cloud Bursting"
Table 6	47	Should "Regional Delivery" renamed / redefined "Multi-Region High Availability" or Multi-Region High Availability
Table 7	48	Might want to include link or extra details about "EINSTEIN 3" - Accelerated (E3A)30 is an intrusion-prevention capability offered by NCPS
5,	56	Please expand EAAS acronym to "Email-as-a-Service" the first time it's used, in each section
1. Introduction	1	The initial versions of the TIC initiative sought to consolidate federal networks and standardize perimeter security for the federal enterprise.' - ZTA moves beyond a perimeter model - should that be addressed in the introduction or corrected?
1	2	TIC: The term “TIC” is used throughout the Federal Government to denote different aspects of the TIC initiative; including the overall TIC program, a physical TIC access point (also known as a Traditional TIC), and a TIC Access Provider (TICAP – see below). This document refers to TIC as an adjective or as the Trusted Internet Connections initiative. - Update to put the definition at the beginning if possible.
4.2.1 Shared Security	9	Details around what data category parts are being managed by the CSP, my understanding is that pure data management resides with the customer ala Agency Managed? (Also the first category of IAM covers a very wide capability) With the split of Application into Middleware and Runtime, this covers a very broad spectrum. My suggestion is to either define the categories and what is not covered or to have less and better defined ?