[redacted]

Cherilyn,

Good afternoon! Attached are my comments There is room for clarification on many of these controls Please let me know if you would like any clarification on these points

CSF 2.0 Subcategory	Feedback
GV.OC-04: Critical objectives capabilities and services that stakeholders expect are determined and communicated (formerly ID.BE-4 and ID.BE-5)	Functionally this is the same as GV.OC-05. This should focus on INTERNAL stakeholders.
GV.OC-05: Critical outcomes capabilities and services that the organization relies on are determined and communicated (formerly ID.BE-1 and ID.BE-4)	Functionally this is the same as GV.OC-04. This should focus on EXTERNAL stakeholders (e.g. third-party providers consultants etc.).
GV.RM-05 Strategic direction describing appropriate risk response options including cybersecurity risk transfer mechanisms (e.g. insurance outsourcing) investment in mitigations and risk acceptance is established and communicated	This needs clarifications on what this actually means. Does this mean a cybersecurity business plan? Is it merely scoped through existing cybersecurity policies & standards? Does it mean a cybersecurity CONOPS?
GV.RM-06: Responsibility and accountability are determined and communicated for ensuring that the risk management strategy and program are resourced implemented assessed and maintained	This needs clarification. Practically this sounds like it is appointing a "senior organizational official (e.g. CISO) to run the organization's cybersecurity strategy and program" If so state that clearly.
GV.RR-03: Roles and responsibilities for customers partners and other third-party stakeholders are established and communicated (formerly ID.AM-6)	Functionally this is redundant with GV.RR-04. This also required clarification. How do you assign "roles and responsibilities" to customers? This should be stated "Cybersecurity-related roles and responsibilities are established and communicated for all relevant stakeholders both internal and external."
GV.RR-04: Roles and responsibilities for suppliers are established documented in contractual language and communicated (formerly ID.AM-6)	See comments on GV.RR-03
GV.PO-02: The same policies used internally are applied to suppliers	This is just bad and needs to be rewritten since a policy is a "high-level statement of management intent" and this is currently stating that you are directly one company force another company to overwrite its management intent. That is unacceptable. This should be focused on controls not policies. This should be stated "Appropriate cybersecurity and data protection controls are included in contracts with relevant third-parties including subcontractors"
ID.AM-01: Inventories of physical devices managed by the organization are maintained	This can better be worded as "Inventories of technology assets managed by the organization are maintained including physical and virtual assets as well as software." Software is a technology asset.
ID.AM-02: Inventories of software and services managed by the organization are maintained	This conflates software and third-parties which needs rewriting 'Inventories of third-party services are maintained"
ID.AM-04: Inventories of external assets and suppliers are maintained	This appears to be redundant with ID.AM-02 if they are both inventorying third-party services and service providers. This is where both ID.AM-02 and ID-AM-04 need clarification/rewriting.
ID.RA-03: Threats both internal and external are identified and recorded	This appears to be conflating the concept of risks and threats. They are different and the section is on risk so it should be a risk catalog. It would make sense to create a new subcategory to make a threat catalog.
ID.RA-09: Processes for receiving analyzing and responding to vulnerability disclosures are established (formerly RS.AN-5)	What is the context of this? Is this a Vulnerability Disclosure Program (VDP) or are you monitoring for unauthorized data exfiltration? This is unclear and needs to be clarified.
PR.AT-03: Awareness and training are provided for third parties with cybersecurity responsibilities (e.g. suppliers partners customers) so they possess the knowledge and skills to perform relevant tasks	This is misguided and needs to be rewritten since it only benefits training companies by expanding the scope of the audience. This should be contractual for third-parties to train their own staff and not one company paying for the training of another company's staff.
PR.AT-04: Awareness and training are provided to senior leaders so they possess the knowledge and skills to govern and lead a cybersecurity risk-aware culture	How is this any different from "role-based" training? They are a role just like cybersecurity staff. Role-based training just needs to focus on the role.
PR.DS-01: The confidentiality integrity and availability of data-at-rest is protected (formerly PR.DS-1 PR-DS.5 PR.DS-6 and PR.PT-2)	In concept this sounds good but is misguided. By throwing in the CIA Triad that is essentially bringing the entire cybersecurity program into scope for how to implement this subcategory. Since this is specifically data at rest it should focus on encryption or alternative physical protections (e.g. physical security).
PR.DS-02: The confidentiality integrity and availability of data-in-transit is protected (formerly PR.DS-2 PR.DS-5)	Same concept as PR.DS-01. Since this is data in transit that is encryption. Therefore speak about encryption since there is no other way to protect data in transit.
PR.DS-10: The confidentiality integrity and availability of data-in-use is protected (formerly PR.DS-5)	This really needs to be re-written. How do you define "data in use" - it is not at rest but that could also mean it is in transit. Therefore you appear to mean that data is being processed. Reword it to state how data is to be protected while it is being processed in an application system and/or service.
PR.PS-01: Configuration management practices are applied (e.g. least functionality least privilege) (formerly PR.IP-1 PR.IP-3 PR.PT-2 and PR.PT-3)	Why not state this clearly as "hardened secure configuration baselines that implement least functionality and least privileges"?
PR.PS-03: Hardware is maintained replaced and removed commensurate with risk	Why not state this a "technology lifecycle management to prevent technical debt accumulation"?
PR.PS-04: Log records are generated for cybersecurity events and made available for continuous monitoring (formerly PR.PT-1)	Why not state this is "Security event logs are generated and forward to a centralized event log repository for review and analysis "?
PR.PS-05: Protective technologies are executed on or within platforms to stop unauthorized software execution	Why not state this as "system configurations prevent the execution and/or installation of unauthorized software"?
PR.PS-06: Backups of platform software are conducted protected maintained and tested	What does this mean to a company that has SaaS or hybrid cloud solutions? This should be focused on "storing

	backup copies of critical software and other security-related information" and provide additional clarity on the expectation.
PR.PS-08: Supply chain security practices are integrated and their performance is monitored throughout the technology product and service life cycle	This is somewhat redundant to GV.RM-02. This really just describes having a C-SCRM program.
PR.IR-01: Response and recovery plans (e.g. incident response plan business continuity plan disaster recovery plan contingency plan) are communicated and maintained (formerly PR.IP-9)	These are hugely different topics Incident Response (IR) Disaster Recovery (DR) & Business Continuity (BC). These should have their own focus at a subcategory level.
PR.IR-03: The organization s computing assets are protected from environmental threats (formerly PR.IP-5)	Where? On prem only? What about remote workers third-parties etc.?
DE.AE-02: Adverse events are analyzed to find possible attacks and compromises	Is this supposed to be Indicators of Compromise (IOC)? If so just call it IOC.
DE.AE-03: Information on adverse events is correlated from multiple sources	Adverse means "undesirable" and indicates something bad happened. From a situational awareness perspective this should be changed to "anomalous" to indicate that there is a potential issue. You do not know if an issue is adverse until it has been analyzed properly. This is where the use of adverse is a poor word choice since in most organizations there is considerable "noise" on the network and monitoring focuses on identifying anomalies that could be adverse. They only are categorized as adverse once the event is analyzed after being flagged as anomalous.
DE.AE-04: The estimated impact and scope of adverse events is determined	Same issue with "adverse" as DE.AE-03
DE.AE-05: Incident alert thresholds are established	It isn't an "incident alert threshold" and is an "event alert threshold" - For example a threshold for a "malware outbreak" is >10 machines that alert on a specific malware signature within a defined timeframe. That is the alerting threshold but it is from a number of unique events that exceeds a predetermined threshold.
DE.AE-06: Information on adverse events is provided to cybersecurity and incident response tools and staff (formerly DE.DP-4)	Same issue with "adverse" as DE.AE-03
DE.AE-07: Contextual information (e.g. cyber threat intelligence inventories security advisories) is integrated into the adverse event analysis	Same issue with "adverse" as DE.AE-03
DE.AE-08: Adverse cybersecurity events are categorized and potential incidents are escalated for triage	Same issue with "adverse" as DE.AE-03
DE.CM-01: Networks and network services are monitored to find adverse cybersecurity events (formerly DE.CM-1 DE.CM-4 DE.CM-5 and DE.CM-7)	Same issue with "adverse" as DE.AE-03
DE.CM-02: The physical environment is monitored to find adverse cybersecurity events	Same issue with "adverse" as DE.AE-03
DE.CM-03 Personnel activity and technology usage are monitored to find adverse cybersecurity events (formerly DE.CM-3 and DE.CM-7)	Same issue with "adverse" as DE.AE-03
DE.CM-06: External service providers and the services they provide are monitored to find adverse cybersecurity events (formerly DE.CM-6 and DE.CM-7)	Same issue with "adverse" as DE.AE-03
DE.CM-09: Computing hardware and software and their data are monitored to find adverse cybersecurity events (formerly PR.DS-6 PR.DS-8 DE.CM-4 DE.CM-5 and DE.CM-7)	Same issue with "adverse" as DE.AE-03
RS.MA-01: The incident response plan is executed (formerly RS.RP-1)	When? The IRP should be executed only when a trigger occurs such as an IOC.
RS.MA-02: Incident reports are triaged and validated (formerly RS.AN-1 and RS.AN-2)	This should come after RS.MA-03 since you need to categorize what you are dealing with (e.g. IOC) to understand how to triage the incident.
RS.MA-03: Incidents are categorized and prioritized (formerly RS.AN-4 and RS.AN- 2)	This should come before RS.MA-02 since you need to categorize what you are dealing with (e.g. IOC) to understand how to triage the incident.
RS.MA-05: Criteria for initiating incident recovery defined and applied	Is this to rename "disaster recovery" as "incident recovery"? This should be clearly defined as Disaster Recovery (DR) since it is different in scope from containing /eradicating an incident (e.g. RS.MI-01 and RS.MI-02). You have incident response that may or may not trigger a larger scale disaster recovery which itself is a subcomponent of broader business continuity operations.

	RS.MI-01 Incidents are contained RS.MI-02 Incidents are eradicated
RS.AN-03: Analysis is performed to determine what has taken place during an incident and the root cause of the incident	This should come after RS.AN-06. An After Action Review (AAR) / Root Cause Analysis (RCA) comes after actions are recorded.
RS.AN-06: Actions performed during an investigation are recorded and the record s integrity and provenance are preserved (formerly part of RS.AN-3)	This should come before RS.AN-03. It occurs before an After Action Review (AAR) / Root Cause Analysis (RCA).
RS.AN-07: Incident data and metadata are collected and their integrity and provenance are preserved	This should be "proper forensic practices are utilized to preserve the integrity of evidence" The current wording is confusing and should focus on applying Federal rules of evidence to protect incident-related data for possible prosecution.
RS.AN-08 Incident magnitude is estimated and validated	This should occur at the same time as RS.AN-03.
RS.AN-09: Incident status is tracked and validated	This should come immediately after RS.MA-01
RS.CO-04: Escalation is coordinated with designated internal and external stakeholders as required by law regulation or policy	"or policy" should be "or contractual obligation" - a contractual obligation with a third-party is what is going to require escalation and reporting.
RC.RP-01: The incident recovery plan is executed	When? The Business Continuity Plan (BCP) should be executed only when a trigger occurs such as a step/component of an IRP that requires recovery.
RC.RP-03 The integrity of backups and other restoration assets is verified before using them for restoration	You are not verifying the integrity of the backups. You are verifying the integrity of the recovered system/service/data following restoration. That is a big difference. The integrity of backups is a component of PR.DS-11
RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	Why not state it as "business continuity planning takes critical mission functions into account for post-incident operations"
RC.RP-05: The integrity of restored assets is verified systems and services are restored and normal operating status is confirmed	Redundant to a properly-worded RC.RP-03
RC.RP-06: Criteria for determining the end of incident recovery are defined and applied and incident-related documentation is completed	Why not state it as "business continuity plans include criteria for determining the end of business continuity operations to resume normal operations"
RC.CO-01: Public relations are managed	Public relations are proactively managed to mitigate potential harm to business operations and/or individuals.

Respectfully,

Tom Cornelius, CISSP, CISA, CRISC, CDPSE, CIPP/US, PCIP, MCITP, MBA
SCF Founder & Contributor
[redacted]

SECURE CONTROLS FRAMEWORK

[redacted]