July 10, 2023

Cybersecurity Framework Draft 2.0 Core - Feedback

Thank you for the opportunity to review the preliminary draft of the NIST Cybersecurity Framework (CSF) 2.0 Core updates. The feedback below was provided by CForum and compiled by Optic Cyber Solutions.

CForum is an association of industry experts driving discussions around information security focused on the major challenges faced by organizations today. Members of CForum are cybersecurity practitioners, leaders, and consultants. As such, our membership has implemented the NIST CSF within their own organizations (e.g., energy sector, transportation sector, technology sector, education sector) as well as partnered with other organizations in leveraging the Framework successfully.

As a community we value the Cybersecurity Framework's simple structure and flexible implementation as it helps to enable cybersecurity improvement and communication across industries. We look forward to supporting the update process in the hopes that this will continue through the 2.0 update, finalization, and release.

1 General Feedback

The sections below describe CForum's perspective and recommendations for the Implementation Examples, the new Govern Function, and the Adverse Event Analysis Category.

1.1 Implementation Examples

We do not feel that it is appropriate for the Implementation Examples to be included in the CSF Core. For clarity, the Implementation Examples are a great idea, and many organizations will benefit from more guidance and examples. However, we believe these examples should be included either as an additional section of the document, or an online repository rather than being built into the Core itself.

The CSF is not expected to be updated sooner than every three to five years and technology, techniques, and methods for implementing the outcomes described in the Subcategories continually change and improve. NIST has already shown that Informative Reference should not be included in the Core as the reference documents update more frequently than the CSF. The lessons learned from the Informative Reference must be applied to the Implementation Examples if the examples are to remain relevant and valid over time.

Additionally, while the introductory text of the CSF v1.1 explained the purpose of the Informative References, many organizations did not understand how to use them. Instead, many organizations, as witnessed by the CForum community, saw them used as a checklist of activities that need to be performed to meet the goals of the Subcategory. We would not want the Implementation Examples to become a checklist or be viewed as a prescribed way for achieving each Subcategory.

NIST is encouraged to continue the process of including Implementation Examples for the CSF Subcategories; however, not as part of the Core. The key customers who will benefit from the implementation examples will be new organizations, or organizations trying to identify best practices to address any gaps in their implementation or adoption. We recommend that the Implementation Examples should be maintained in an online repository or separate document where they can be updated as technologies and methods improve. Ideally, NIST could facilitate a moderated, crowd-sourced, environment where Implementation Examples could be maintained and expanded by industry for all types of organizations and technologies including Operational Technologies.

1.2 Govern Function

We agree that governance is important and that it should be considered as a key component of a cybersecurity program. However, our membership is concerned that adding Govern as an additional Function may create confusion among smaller organizations or those with immature cybersecurity programs.

Implementing formal governance programs for a small business presents three key challenges: resource limitations, lack of awareness and expertise, and scalability. Limited budgets and personnel make it difficult to allocate resources for formally defined governance practices, necessitating strategic resource management. The lack of cybersecurity awareness and expertise requires investing in training and building a cybersecurity-focused culture. Additionally, scalability poses a challenge as small businesses experience growth and operational changes, requiring flexible governance frameworks.

We propose that if Govern is added as a new Function that there is consideration for how to communicate this change. Much of our membership has spent a significant amount of time and resources training their team and leadership on the current 5 Functions and building out their programs around these concepts. Adding this new Function will create a need to retrain and educate these individuals so any resources to aid in this re-training would be very helpful to minimize confusion and reduce rework.

Additionally, we proposed that if Govern is added as a new Function, that it is depicted in the same manner as the existing 5 Functions, as seen in Figure 1 below. There have been discussions throughout the community around depicting the Govern Function as a “wrap-around” or in the center of the existing image. However, we believe that if this was done, that it would increase confusion amongst organizations, specifically small businesses, around the meaning of a “Function.” Therefore, we believe all Functions should be depicted in the same format. In adding the Govern Function as “another piece of the pie” this would illustrate that governance should be handled in the same manner as the existing Functions today. Adding the new Function in this way would help to minimize the amount of work and training required to educate staff and leadership on the change.

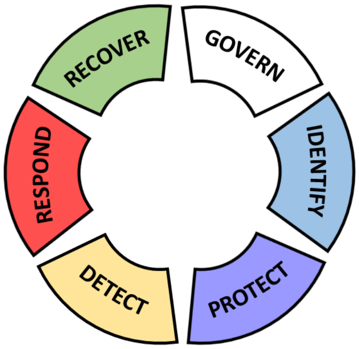

Figure 1 Proposed Depiction of Functions for CSF 2.0

1.3 Adverse Event Analysis Category

The Detect Function included a new Category called “Adverse Event Analysis (DE.AE)”. This Category introduces the term “adverse events” to the Core which has created confusion amongst our membership. While CForum members appreciate and understand the outcome-based objectives defined by the CSF Core, defining that only adverse events must be analyzed, reviewed, or scoped causes confusion as this seems to exclude any “potentially” adverse events. The term adverse implies harmful or unfavorable; therefore, for Subcategories such as “DE.AE-02: Adverse events are analyzed to find possible attacks and compromise”, it is viewed that only events that have already harmed the organization are analyzed. Organizations should be encouraged to take a more proactive approach to security by analyzing potentially adverse events and not only those shown to already be adverse.

The Subcategory “DE.AE-03: Information on adverse events is correlated from multiple sources” clearly states that only the adverse events need to be correlated. CForum members have found that correlating routine events (e.g., user physically badging into one authorized location while successfully logging onto a workstation in a separate physical location) can provide greater insight into a potential attack. Only correlating adverse events would not detect when these suspicious or harmful acts are occurring.

Additionally, the term “Adverse Event” is used in multiple contexts throughout the Core update. It is referenced in places as “Adverse Cybersecurity Event” (e.g., DE.AE-08, DE.CM-06), “Adverse Event” (e.g., DE.AE-02, DE.AE-07), and “Potential Adverse Event” (e.g., DE-CM). The multiple contexts add confusion on which types of events are to be analyzed. Should it only be cybersecurity related adverse events, any confirmed adverse event, or any event with potential adverse impact?

Version 1.1 of the CSF Core provided flexibility for organizations to review events to determine if a potential adverse activity was occurring. CForum members found this flexibility important to appropriately tune and configure monitoring technologies and processes. Consider redefining the use of the term “Adverse” for only those areas where harmful activities have occurred. Alternatively, consider using terms such as “events”, “potential adverse events”, and “adverse events” based on the context of the outcome being described.

2 Specific Subcategory Comments

The comments included in the Table 1 below focus on proposed text updates to enhance clarity, considerations for change, or questions regarding the intent of a Category or Subcategory.

To assist with the review of the inputs included in the table below, proposed text changes in the “CForum Proposed Text” column have been identified via track changes.

Table 1. Specific Subcategory Comments

#	CSF 2.0 Draft Text	CForum Proposed Text	Considerations/ Questions
1.	GV.OC-04: Critical objectives, capabilities, and services that stakeholders expect are determined and	Critical objectives, capabilities, services, and dependencies that stakeholders expect are	Proposing revisions to re-add the dependencies portion of the text as dependencies are commonly overlooked during implementation.

#	CSF 2.0 Draft Text	CForum Proposed Text	Considerations/ Questions
	communicated (formerly ID.BE-4 and ID.BE-5)	determined and communicated	
2.	GV.OC-04: Critical objectives, capabilities, and services that stakeholders expect are determined and communicated (formerly ID.BE-4 and ID.BE-5)	Critical objectives, capabilities, and services that internal and external stakeholders expect from the organization are determined and communicated	Proposing revisions for clarity with the assumption the text excerpt "…that stakeholders expect.." is intended to address how both internal and external stakeholders rely on the organization.
3.	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	Strategic direction describing appropriate risk response options is established and communicated	Proposing revisions to include all risk options by not specifying the types of options available. The current Subcategory implies that risk avoidance and exploitation are not appropriate.
4.	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	N/A	Consider removing this Subcategory as it is addressed by the new GV.RR Category. Specifically, GV.RR-01: "Organizational leadership takes responsibility for decisions associated with cybersecurity risks and establishes a culture that is risk-aware, behaves in an ethical manner, and promotes continuous improvement" appears to cover this topic area.
5.	GV.RM-07: Risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	N/A	Proposing that this Subcategory is not needed with the new ID.IM Category which covers "Improvements to organizational cybersecurity risk management processes and activities are identified."
6.	GV.RM-08: Effectiveness and adequacy of cybersecurity risk management strategy and results are assessed and reviewed by organizational leaders	N/A	Proposing that this Subcategory is not needed with the new ID.IM Category which covers "Improvements to organizational cybersecurity risk management processes and activities are identified."

#	CSF 2.0 Draft Text	CForum Proposed Text	Considerations/ Questions
7.	GV.RR-01: Organizational leadership takes responsibility for decisions associated with cybersecurity risks and establishes a culture that is risk-aware, behaves in an ethical manner, and promotes continuous improvement	Organizational leadership takes responsibility and accountability for decisions associated with cybersecurity risks and establishes a culture that is risk-aware, behaves in an ethical manner, and promotes continuous improvement	Proposing revisions to include accountability as leadership is ultimately answerable for decisions associated with cybersecurity risk.
8.	GV.RR-03: Roles and responsibilities for customers, partners, and other third-party stakeholders are established and communicated (formerly ID.AM-6)	N/A	This Subcategory appears to be redundant with GV.RR-04: “Roles and responsibilities for suppliers are established, documented in contractual language, and communicated.”, and the breakout of each party (customers, partners, and other third-party stakeholders) is inconsistent with how PR.AT is organized. The intent of using this alignment appears to be purposeful but is unclear. Consider breaking out the named parties in a consistent way or otherwise revising for additional clarity.
9.	GV.PO-02: The same policies used internally are applied to suppliers	Policies used internally are applied to suppliers, as appropriate, based on risk	Proposing revisions to provide flexibility as the current text may lead to situations that could be either too restrictive or not restrictive enough based on the scenario. For example, different risk tolerances based on the role of specific suppliers may lead to a different need and outcome.
10.	GV.PO-03: Policies and procedures are reviewed, updated, and communicated to reflect changes in requirements, threats, technology, and organizational mission	N/A	This text appears to be a maturity step and not an outcome statement. If it is included as written, it may imply that other Categories do not have to be reviewed and updated because there isn't a corresponding subcategory.

#	CSF 2.0 Draft Text	CForum Proposed Text	Considerations/ Questions
			Additionally, these types of activities appear to be covered by Improvement (ID.IM). Consider revising to ensure alignment.
11.	ID.AM-01: Inventories of physical devices managed by the organization are maintained	Inventories of physical devices are maintained	Proposing a more concise outcome to minimize confusion during implementation. The current text implies that if the devices are managed by an external party, that they would be out of scope.
12.	ID.AM-02: Inventories of software and services managed by the organization are maintained	Inventories of software and services are maintained	Proposing a more concise outcome to minimize confusion during implementation. The current text implies that if the software and services are managed by an external party (e.g., MSP), that they would be out of scope.
13.	ID.AM-07: Sensitive data and corresponding metadata are inventoried and tracked	Data and corresponding attributes are inventoried and tracked	Proposing revisions to encompass data wholistically (e.g., non-sensitive, sensitive, related attributes/metadata, etc.) as some data may not be sensitive, but important or critical to maintaining operations.
14.	ID.AM-08: Systems, devices, and software are managed throughout their life cycle, including pre-deployment checks, preventive maintenance, transfers, end-of life, and disposition (formerly PR.DS-3, PR.IP-2, PR.MA-1, and PR.MA-2)	N/A	Consider moving this Subcategory to Protect as it is not focused on identification, but protection capabilities.
15.	ID.RA-01: Vulnerabilities in first-party and third-party assets are identified, validated, and recorded (formerly ID.RA-1 and DE.CM-8)	Vulnerabilities (i.e., logical, physical) in first-party and third-party assets are identified, validated, and recorded	Proposing revisions to include considerations for both technical and physical vulnerabilities.

#	CSF 2.0 Draft Text	CForum Proposed Text	Considerations/ Questions
16.	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources ID.RA-03: Threats, both internal and external, are identified and recorded	N/A	Consider removing ID.RA-02 since the outcome of achieving ID.RA-03 could logically be addressed by performing the activities included in ID.RA-02.
17.	ID.RA-07: Changes are managed, assessed for risk impact, and recorded (formerly part of PR.IP-3)	Changes and exceptions are managed, assessed for risk impact, and recorded	Proposing revisions to include exceptions as there is a concern that concept of general change control may be lost by only having a portion of PR.IP-3, which focused on configuration change control processes, incorporated into this Subcategory. Consider realigning this Subcategory to Platform Security (PR.PS) as PR.PS-01 addresses applying configuration management practices.
18.	ID.RA-10: Exceptions to security measures are reviewed, tracked, and compensated for	N/A	Consider the proposed revisions to ID.RA-07 (above) and removing ID.RA-10. The proposed revisions to ID.RA-07 (above) along with PR.PS appear to address a wholistic change management process.
19.	ID.IM-01: Continuous evaluation, including through reviews, audits, and assessments (including self-assessments), is applied to identify opportunities for improvement across all Framework Functions	Continuous evaluation, including through reviews, audits, and assessments (including self-assessments), is applied to identify opportunities for improvement	Proposing revisions to remove ”across all Framework Functions” text. This is understood without being stated explicitly and is inconsistent with language used in other Subcategories.
20.	ID.IM-03: Improvements for processes and activities across all Framework Functions are identified based on lessons learned (formerly PR.IP-7, PR.IP-8, DE.DP-5,	Improvements for processes and activities are continuously implemented based on lessons learned	Proposing revisions to change “identified” to “implemented” so that the outcome includes making the improvement and remove ”across all Framework Functions” as this is understood without being

#	CSF 2.0 Draft Text	CForum Proposed Text	Considerations/ Questions
	RS.IM-1, RS.IM-2, and RC.IM-2)		stated explicitly. The current text appears to be a maturity improvement and not an outcome statement.
21.	PR.AA-01: Identities and credentials for authorized users, processes, and devices are managed by the organization (formerly PR.AC-1)	Identities and credentials for authorized users, processes, and devices are issued, managed, and revoked by the organization	Proposing revisions to address the full management lifecycle of identities and credentials.
22.	PR.AA-04: Federated assertions are generated, protected, conveyed, and verified	N/A	This Subcategory appears to be an overly technical and mature Subcategory. Consider revising to focus on the commons methods (e.g., Security Assertion Markup Language (SAML), OpenID Connect, OAuth) when using federated identity systems.
23.	PR.AA-06: Account activities and access events are audited and monitored to enforce authorized access (formerly PR.AC-1 and PR.AC-3)	N/A	This Subcategory appears to be more aligned with a Detection outcome vs Protect. Consider revising to align more with the Detect Function.
24.	PR.AT-01: Awareness and training are provided for users so they possess the knowledge and skills to perform relevant tasks (formerly PR.AT-1 and RS.CO-1)	Users are provided awareness and training to ensure they possess the knowledge and skills to perform relevant tasks	Proposing revisions for clarity to focus on the subjects of the training (i.e., users).
25.	PR.AT-02: Awareness and training are provided for users with elevated privileges so they possess the knowledge and skills to perform relevant tasks (formerly PR.AT-2 and PR.AT-5)	Users with elevated privileges or security focused roles are provided awareness and training to ensure they possess the knowledge and skills to perform relevant tasks	Proposing revisions for clarity to focus on the subjects of the training (i.e., users with elevated privileges).
26.	PR.AT-03: Awareness and training are provided for third parties with cybersecurity responsibilities (e.g., suppliers, partners, customers) so they possess	Third parties with cybersecurity responsibilities (e.g., suppliers, partners, customers) are provided awareness and training to ensure they possess the	Proposing revisions for clarity to focus on the subjects of the training (i.e., third parties).

#	CSF 2.0 Draft Text	CForum Proposed Text	Considerations/ Questions
	the knowledge and skills to perform relevant tasks	knowledge and skills to perform relevant tasks	
27.	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	Senior leaders are provided awareness and training to ensure they possess the knowledge and skills to govern and lead a cybersecurity risk-aware culture	Proposing revisions for clarity to focus on the subjects of the training (i.e., senior leaders).
28.	PR.PS-02: Software is patched, updated, replaced, and removed commensurate with risk (formerly PR.IP-12)	Software vulnerabilities are managed (e.g., patched, updated, replaced, removed, mitigated) commensurate with risk	Proposing revisions to allow for mitigations, such as addressing through compensating controls when a patch cannot be applied.
29.	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	Physical vulnerabilities are managed (e.g., maintained, replaced, removed, mitigated) commensurate with risk	Proposing revisions to include broader physical vulnerabilities (e.g., such as unlocked doors) as hardware only may be too limiting in scope.
30.	PR.PS-08: Supply chain security practices are integrated and their performance is monitored throughout the technology product and service life cycle	Supply chain security practices are integrated throughout the technology product and service life cycle	Proposing revisions for clarity with the assumption that the review of supplies performance is performed in Protect. Specifically, ID.SC-04: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations Consider moving this Subcategory to ID.SC or moving ID.SC-04 to this Category for consistency and consolidation.
31.	PR.IR-02: The organization's networks and environments are protected from unauthorized logical access and usage (formerly PR.AC-3, PR.AC-5, PR.DS-7, and PR.PT-4)	Networks and environments are protected (e.g., segmented, separated) from unauthorized logical access and usage	Proposing revisions to scope in additional protection details as it appears that much of the specificity from the incorporated Subcategories has been lost.

#	CSF 2.0 Draft Text	CForum Proposed Text	Considerations/ Questions
32.	PR.IR-03: The organization's computing assets are protected from environmental threats (formerly PR.IP-5)	The organization's assets are protected from environmental threats	Proposing revisions for clarity as "computing" may be an unnecessarily limiting term. For example, one could argue that storage would not necessarily be considered a computing asset in a cloud-based modality.
33.	DE.AE-03: Information on adverse events is correlated from multiple sources	Information on potentially adverse events is correlated from multiple sources	Proposing revisions for clarity on adverse events. As written, this Subcategory assumes a level of maturity that would require someone to NOT look at an event unless it is explicitly adverse. For example, two valid login attempts from different physical locations are not adverse until correlated, and realized, that the same user can't be in two different locations at once. Additionally, during the Detect Function, it is not yet known what is adverse.
34.	DE.AE-08: Adverse cybersecurity events are categorized and potential incidents are escalated for triage	Adverse cybersecurity events are categorized and potential incidents are escalated for response triage	Proposing revisions for clarification to ensure the reader realizes that the events are triaged for response activities rather than determination of whether the event is adverse.
35.	Continuous Monitoring (DE.CM)	N/A	Consider rearranging to move the Continuous Monitoring (DE.CM) Category before the Adverse Event Analysis (DE.AE) Category This realignment will support a more logical process flow of monitoring and identifying events before the adverse event analysis is conducted.
36.	DE.CM-01: Networks and network services are monitored to find adverse cybersecurity events (formerly	Networks and network services are monitored to find potentially adverse cybersecurity events	Proposing revisions for clarity as during the Detect Function, it is not yet known what is adverse.

#	CSF 2.0 Draft Text	CForum Proposed Text	Considerations/ Questions
	DE.CM-1, DE.CM-4, DE.CM-5, and DE.CM-7)		
37.	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)	External service provider activities and the services they provide are monitored to find adverse cybersecurity events	Proposing revisions with the assumption that the intent is to scope out the external service provider (e.g., Microsoft) and focus on the provided activities and services (e.g., O365) provided by the service provider.
38.	RS.MA-02: Incident reports are triaged and validated (formerly RS.AN-1 and RS.AN-2)	Reports of potential incidents are triaged and validated	Proposing revisions to include “potential incident” to align with DE.AE-8.
39.	RS.MA-04: Incidents are escalated or elevated as needed (formerly RS.AN-2)	N/A	The intent of this Subcategory appears to be focused on incident communication and awareness which is addressed by RS.CO-4 “Escalation is coordinated with designated internal and external stakeholders, as required by law, regulation, or policy.” Consider removing this Subcategory due to redundancy.
40.	RS.AN-03: Analysis is performed to determine what has taken place during an incident and the root cause of the incident	Analysis is performed to determine the details (e.g., systems affected, files breached) of the incident and the root cause of the incident	Proposing revisions to provide clarification examples of “what has taken place.” As written, this text could be reasonably interpreted to mean different things based on context.
41.	Incident Recovery Plan Execution (RC.RP): Restoration activities are planned and performed to ensure full operational availability of systems and services affected by cybersecurity incidents	Restoration activities are performed to ensure full operational availability of systems and services affected by cybersecurity incidents	Proposing revisions to remove planning activities as the creation and maintenance of the recovery plan is addressed in PR.IR-01 “Response and recovery plans (e.g., incident response plan, business continuity plan, disaster recovery plan, contingency plan) are communicated and maintained”.
42.	Incident Recovery Plan Execution (RC.RP): Restoration activities are planned and performed to ensure full operational	Incident Recovery Plan Execution (RC.RP): Restoration activities are planned and performed to ensure operational availability	Proposing revisions to remove “full” to better align with the referenced Subcategories.

#	CSF 2.0 Draft Text	CForum Proposed Text	Considerations/ Questions
	availability of systems and services affected by cybersecurity incidents	of systems and services affected by cybersecurity incidents	This Category description states "…ensure full operational availability...", however, both RC.RP-04 and RC.RP-06 allow for the determination of operational norms, which may not include full recovery of a system.
43.	RC.RP-06: Criteria for determining the end of incident recovery are defined and applied, and incident-related documentation is completed	Criteria for determining the end of incident recovery is applied and incident-related documentation is completed	Proposing revisions to remove the "defined" portion of the text as it's addressed in Protect. Specifically, PR.IR-01: Response and recovery plans (e.g., incident response plan, business continuity plan, disaster recovery plan, contingency plan) are communicated and maintained.

3 Editorial Subcategory Comments

The comments included in the Table 2 below focus on minor grammatical edits and do not impact the perceived intent of the relevant Subcategory. To assist with the review of the inputs included in the table below, proposed text changes have been identified via track changes.

Table 2 Editorial Subcategory Comments

#	CSF 2.0 Draft Text	CForum Proposed Text	Rationale
1.	RS.MA-05: Criteria for initiating incident recovery defined and applied	Criteria for initiating incident recovery is defined and applied	Proposing minor text update: "…is defined…" to address missing word.
2.	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)	Actions performed during an investigation are recorded and the records' integrity and provenance are preserved.	Proposing minor text update: "…records' integrity" to broaden for multiple records.

4 Additional Considerations

While NIST specifically requested feedback on the proposed Core update, the CForum community felt it important to provide considerations for the other aspects of the CSF. The following subsection provides a recommendation for NIST to consider clarifying the terminology around Profiles.

4.1 Framework Profiles

Many types of Profiles have been developed since the creation of the CSF. Some of these Profiles define technologies in place, others highlight comprehensiveness of capabilities, and still others define an overview of current capabilities. While each of these Profile Types are helpful for specific use cases, we've found that there can be confusion around the breadth of what could be classified as a Profile and recommend defining these Profile Types.

We've included a survey of Profile Types, below in Table 3, that our community has seen in use and provided examples from NIST's "Examples of Framework Profile" webpage, where possible to help illustrate the differences. NIST is encouraged to categorize the current, and future, Profiles listed on NIST's website using the Profile Types defined below to allow organizations to quickly identify the Profile Type to meet their needs.

Table 3 Profile Types

#	Name	Profile Types	Value	Example
1	Sector Profile	Prescribe sector specific requirements (e.g., alignment of controls, drive prioritization)	Understand tailored – sector/industry specific guidance	Maritime Bulk Liquid Transfer, Financial Sector, Manufacturing, Offshore Operations, Passenger Vessel, Election Infrastructure (draft)
2	Performance Profile	Indicate completeness of capabilities or progress towards targets (e.g., maturity level, heat map, Harvey balls, percentage)	Understand sufficiency of capability or differential from targets	Intel, UoC BSD
3	Overlay Profile	Describes specific implementation guidance for preventing common threats or implementing the CSF for specific types of technology (e.g., Ransomware, IOT, AI).	Understand how different types of technology can be layered on top of the CSF	Ransomware Risk Management (NISTIR 8374), Cybersecurity Framework Botnet Threat Mitigation Profile - Cybersecurity Coalition, Cybersecurity Framework DDoS Threat Mitigation Profile
4	Summary Profile	Describe capabilities through narrative (e.g., short elevator pitch, robust definition)	Understand cybersecurity program activities through description of capabilities	Optic Cyber Solutions