NIST Interagency Report
NIST IR 8623 ipd

Cybersecurity Framework 2.0 Community Profile for Federal Agency Open Radio Access Network (O-RAN) Deployment

Initial Public Draft

Scott Rose

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8623.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Interagency Report
NIST IR 8623 ipd

Cybersecurity Framework 2.0 Community Profile for Federal Agency Open Radio Access Network (O-RAN) Deployment

Initial Public Draft

Scott Rose
Wireless Networks Division
Communication Technology Lab

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8623.ipd

September 2026

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added upon final publication]

How to Cite this NIST Technical Series Publication
Rose S (2026) Cybersecurity Framework 2.0 Community Profile for Federal Agency Open Radio Access Network (O-RAN) Deployment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8623 ipd. https://doi.org/10.6028/NIST.IR.8623.ipd

Author ORCID iDs
Scott Rose: 0000-0002-3105-7427

Public Comment Period
September 17, 2026 – November 2, 2026

Submit Comments
oran-cybersecurity@nist.gov

National Institute of Standards and Technology
Attn: Wireless Networks Division, Communication Technology Laboratory
100 Bureau Drive (Mail Stop 8920) Gaithersburg, MD 20899-8920

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8623/ipd, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA)

Abstract

The NIST Cybersecurity Framework (CSF) 2.0 is a tool to help organizations manage risk in their operations. The CSF can also be used to develop a profile for communities that have similar risks in their operations. These community profiles can help individual members adapt the CSF to their own internal operations, while also providing a common sense of risk seen by all members of the community. This community profile is aimed at federal agencies wishing to deploy an Open Radio Access Network (Open RAN) as part of their infrastructure. This profile aids agency cybersecurity managers in integrating an Open RAN component to their infrastructure by providing an evaluation of threats and resources. These resources may help cybersecurity managers in producing their internal CSF organizational profile or cybersecurity strategy with regards to their Open RAN deployment.

Keywords

Cybersecurity Framework; CSF; Open RAN; O-RAN; risk; threats.

Table of Contents

List of Figures

Acknowledgments

This report is based on work that was funded by the Department of Homeland Security (DHS) Science & Technology Directorate.

Note to Reviewers

This profile uses several reports and specification documents developed by the O-RAN ALLIANCE. Some of these publications are likely to be revised. The references are meant to be an aid to developing a strategy and claimed conformance to a given specification may not mean that the CSF outcome is fully met. Comments should focus on the description of the profile and the references but not the content of those references. Comments about those documents should be submitted to the relevant venues (NIST publications or the O-RAN ALLIANCE).

1. Introduction

The Cybersecurity Framework (CSF) 2.0 "…offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization…to better understand, assess, prioritize and communicate its cybersecurity efforts [1]." Initial versions of the CSF were aimed at organizations that operated critical infrastructure. This update expanded the framework to make it easier to apply the CSF more industry sectors. This includes US Federal agencies, which were mandated to use the CSF in their cybersecurity management plans in EO 13800 [2].

The CSF is broken down into 6 core functions, which in turn are broken down into categories and subcategories (see Fig. 1). Each of these subcategories contains these high-level cybersecurity outcomes but does not mandate the technology or techniques that should be used to achieve the outcome. Individual technology or industry sectors and individual entities tailor their own solutions to the given outcome.

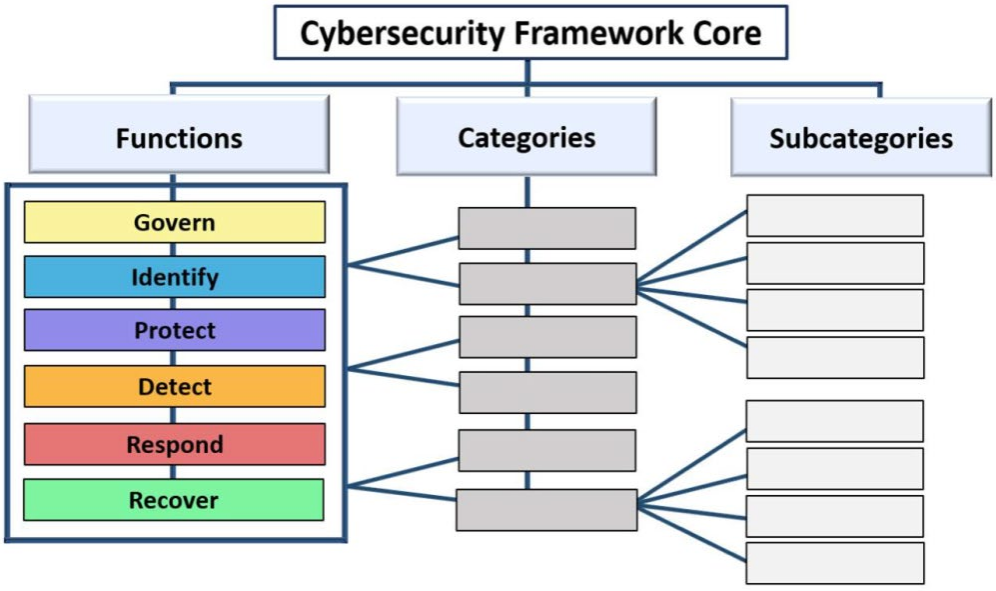

Figure 1: CSF 2.0 Functions, Categories and Subcategories (from [1])

1.1. Cybersecurity Framework Profiles

There are several ways to apply the CSF, depending on the subject. One way is through profiles, which can apply to a single organization (called an "organizational profile") or to a group of organizations in a specific industry or sector (called a "community profile"). An organizational profile is used within an enterprise to measure and plan its cybersecurity posture and processes. A community profile is one designed to apply to a group of organizations that are in the same industry or similar in some way [3]. As community profiles are designed to apply to an entire group, the goal is not to propose a single process or technology solution, but prioritize outcomes based on common threats the group face. Members of the group can then use the

community profile to prioritize and plan their individual organization's profile. The organization profile is then used to develop the organization's cybersecurity policies and strategy and measure progress towards the outcomes.

2. Open Radio Access Networks

Modern mobile telecommunication networks are divided into two logical segments: the Radio Access Network (RAN) and the mobile core. The RAN is responsible for managing the connection of User Equipment (UEs) to the network via a radio link to the core network (and ultimately the Internet). This includes functions like network resource access, management and mobility. With the advent of 5G mobile networks, there has been an effort to redefine the RAN as a set of disaggregated components with standardized interfaces referred to as an Open RAN (O-RAN). O-RAN would allow mobile network operators (MNOs) to build infrastructure using components from different vendors that interoperate. Building mobile networks on more open, standardized architectural components will continue into 6G and beyond. The O-RAN ALLIANCE is the organization formed to define the components and interfaces for Open RAN [4] as shown in Fig 2 below:

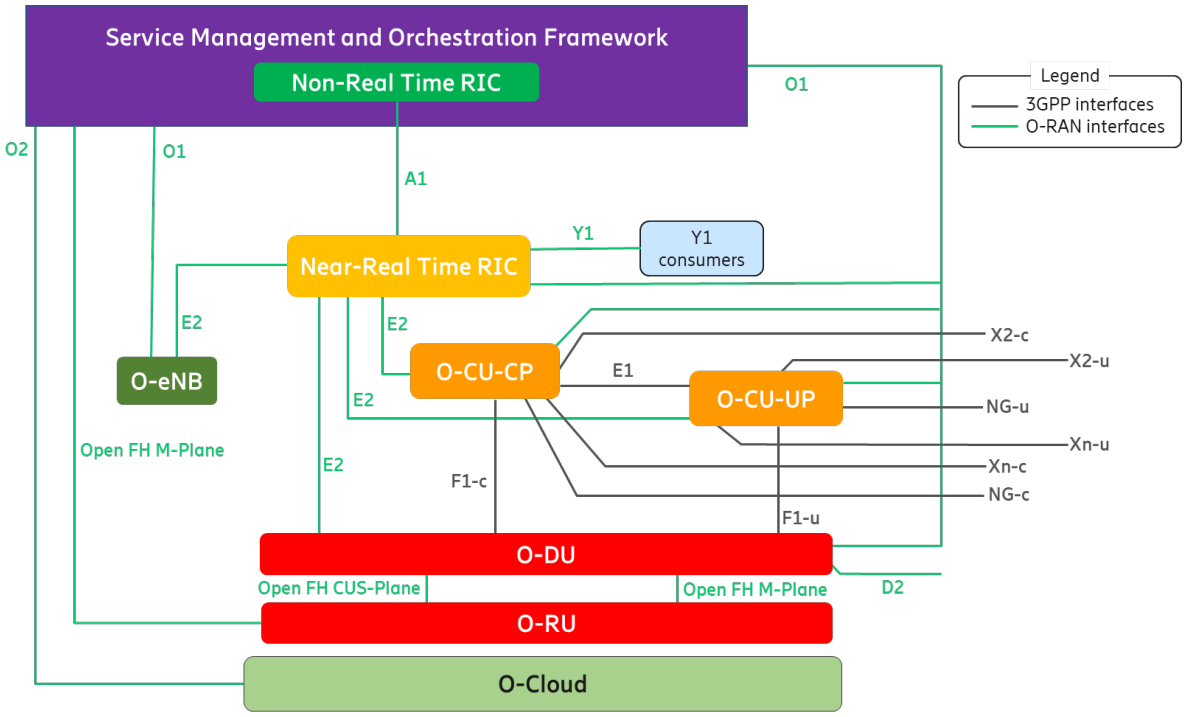

Figure 2: O-RAN Logical Architecture (from [4])

One aspect of this O-RAN is that, apart from the actual Radio Unit (RU), part or all the RAN is composed of software components hosting O-RAN specified services. This means that commodity IT infrastructure can be used to host O-RAN components. This can reduce cost and complexity and can increase reliability as components can be operated as cloud native deployments. This also enables the RAN to be updated or modified more quickly than with dedicated hardware or physical appliances used to support the network infrastructure.

One of the advantages of this use of commodity IT components is that it is easier and deploy custom RAN deployments for customers with specific requirements as private 5G RAN. This

means an organization (such as a federal agency) can deploy a 5G RAN as part of their network infrastructure. Agencies then include the 5G RAN deployment in their IT security planning.

2.1. O-RAN ALLIANCE Security Specifications and Reports

The O-RAN ALLIANCE produces two major categories of publications: Technical Specifications (TS) and Technical Reports (TR). TS documents features and requirements that are to be present in O-RAN products. It is intended that “O-RAN components” implement some or all relevant specifications and may have test results that prove conformance to specifications. TR documents are reports that are not standards or include implementation requirements but can include information on O-RAN operation, architecture that may be useful in deployments.

This profile includes references to both O-RAN ALLIANCE TS and TR documents. The references to report documents are for informational use only. TRs often contain guidance that could be useful when preparing security plans and policies for federal RAN usage. Then should not be used as hard requirements for products however, as O-RAN products only need to implement the necessary requirements found in TS documents.

3. How to Use this Profile

This CSF community profile differs from others in that it attempts to provide references and resources to integrate a private RAN into existing framework documents and security plans. There will never be an agency that solely operates a RAN for its own sake, but as part of larger agency infrastructure. This profile is aimed to provide pointers to information that is useful in producing security plans when a RAN is part of the system being documented.

The profile has additional columns beyond the standard template of community CSF profiles [3] to provide these references. They are listed below with a description of how they may be used to when preparing a larger organizational profile, or other types of agency cybersecurity planning.

3.1. Outcome

This column is unchanged from the CSF 2.0 community profile template [5] this lists the outcomes for each family of outcomes in CSF 2.0. This is also listed in the guide to producing community profiles [3] and would appear in any community profile.

3.2. Priority

This column is also present in the CSF 2.0 community profile template [5] and the description can be found in the guide to community profiles [3]. This is used in a similar way as what is intended for community profiles. The priority for a given outcome is based on comparing O-RAN ALLIANCE identified threats [6] and any other relevant documents such as the Enduring Security Framework (ESF) documents on 5G. Some policies or guidance that applies only to federal agencies may also affect the priority, in that agencies risk management policies may increase the priority value over what a private industry O-RAN deployment may take as the priority.

The actual priority for an agency may differ, as these are focused solely on relevant O-RAN components. This would not take account any other components, use case, data sent over the RAN, etc.

3.3. O-RAN ALLIANCE Risk Score (Rationale)

This column gives the assumed priority according to the O-RAN ALLIANCE Threat Analysis TR [6]. This focuses on the threats as identified by the O-RAN ALLIANCE and does not take any other factor into analysis. This varies based on the O-RAN component, as the threat to some components would result in larger impact than others.

The O-RAN ALLIANCE only makes specifications for components and does not specify how they are deployed, managed and operated. This results in some values being listed as “OutOfScope”. This means the given outcome deals with operational concerns and cannot be addressed by specific O-RAN ALLIANCE produced specifications. This does not mean that it is not a concern

for a deployment. It could be a serious concern to a federal agency but one that cannot be addressed by a standard but depends on the individual deployment.

3.4. Relevant O-RAN ALLIANCE Specifications or Technical Reports

This column gives any reference to specific O-RAN ALLIANCE published TS or TR documents that may help a federal cybersecurity manager to develop a response to meet the given outcome. If it is a specification, it indicates that there could be some feature or capability in some O-RAN components that may support achieving this outcome. If it is to a report, it should be used to provide information or recommendations for meeting the outcome but does not mean that there is a specific feature or capability in O-RAN components that helps meet this outcome.

3.5. Other Federal Guidance

This column gives information or references to other guidance aimed at federal agencies that may support the outcome. This will usually be NIST publications but also include known policy directives such as CISA Binding Operational Directives (BoDs) or similar. NIST guidance publications are meant to assist agency plans to address the outcome or refer to relevant control families in NIST SP 800-53r5 [7] that may be included in an agency's RMF process. Agencies should consider the general mapping of CSF 2.0 to NIST SP 800-53r5[1], but some tailoring may be required to include related controls that support a given outcome for the O-RAN deployment. It should not be assumed that references to CISA or other agency produced policy documents always apply. It would be up to the security team in the agency to review if, and how, an O-RAN deployment would fall under the policy.

[1] Spreadsheet with mapping at https://csrc.nist.gov/csrc/media/Projects/olir/documents/submissions/Cybersecurity_Framework_v2-0_Concept_Crosswalk_800-53_final.xlsx (Accessed Aug 20, 2026)

4. Conclusion

The NIST CSF is a tool to help organizations evaluate, plan and manage risk with IT operations within their enterprise. The CSF can be used to produce a profile to help a given community in developing their own internal plans around the CSF. This community profile should provide a risk analysis and prioritize CSF outcomes based on the threat model of the community. This community profile can then be used by community members to inform and tailor an internal profile for risk management.

This document contains a community profile for federal agencies that wish to deploy O-RAN as part of their enterprise network infrastructure. O-RAN may provide certain advantages over other wireless network technologies but like all networking technologies, bears risk as well. This profile attempts to go further than simply prioritizing outcomes to include references to aid administrators and planners in addressing a given outcome. These references include specifications and reports published by the O-RAN ALLIANCE as well as publications from NIST and other federal sources that may apply to specific federal agency O-RAN deployments.

This profile is not meant to be the sole input to an agency's use of O-RAN. That will ultimately depend on the role of the O-RAN deployment and the types of information transmitted during operation. This profile is only meant as a starting point for an agency when performing a full risk analysis of a specific O-RAN deployment as part of their infrastructure

References

[1] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[2] Executive Order 13800 (2017) Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. (The White House, Washington, DC) DCPD-201700327, May 11, 2017. https://www.govinfo.gov/app/details/DCPD-201700327

[3] Pascoe C, Snyder JN, Scarfone K (2024) NIST Cybersecurity Framework 2.0: A Guide to Creating CSF 2.0 Community Profiles. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 32 ipd. https://doi.org/10.6028/NIST.CSWP.32.ipd

[4] O-RAN ALLIANCE (2025) *O-RAN Architecture Description*. Versions R004-v14. https://specifications.o-ran.org/specifications

[5] National Institute of Standards and Technology (2026) "CSF_2-0_community_profile_template_draft" (Microsoft Excel). Available at https://www.nccoe.nist.gov/sites/default/files/2024-06/CSF_2-0_community_profile_template_draft.xlsx

[6] O-RAN Alliance (2025) *O-RAN Security Threat Modeling and Risk Assessment*. O-RAN ALLIANCE Technical Report. Available at https://specifications.o-ran.org/specifications

[7] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[8] O-RAN ALLIANCE (2025) Application Service Descriptor Specification. Versions R004-v02.00. Available at https://specifications.o-ran.org/specifications

[9] ETSI GS NFV-IFA 011 -V4.2.1 - Network Functions Virtualization(NFV) Release 4; Management and Orchestration; VNF Descriptor and Packaging Specification. (ETSI Sophia Antipolis Cedex - FRANCE). Available at https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/011/04.02.01_60/gs_NFV-IFA011v040201p.pdf

[10] O-RAN ALLIANCE (2025) O-RAN ALLIANCE Security Update 2025. Available at https://www.o-ran.org/blog/o-ran-alliance-security-update-2025

[11] O-RAN ALLIANCE (2025) Security Requirements and Controls Specification 15.0 Versions R005-v15.00. Available at https://specifications.o-ran.org/specifications

[12] Licata J, McWhite R, Calloway L, Gilbert D, Anderson M, Snyder J, Miller J (2026) Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18r2. https://doi.org/10.6028/NIST.SP.800-18r2

[13] Cybersecurity and Infrastructure Security Agency (2022) "BOD 23-01: Implementation Guidance for Improving Asset Visibility and Vulnerability Detection on Federal Networks" Available at https://www.cisa.gov/news-events/directives/bod-23-01-implementation-guidance-improving-asset-visibility-and-vulnerability-detection-federal

[14] O-RAN ALLIANCE (2026) Study on Continuous Security Monitoring R005-v02.00. Available at https://specifications.o-ran.org/specifications

[15] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[16] O-RAN ALLIANCE (2026) O-RAN ALLIANCE Coordinated Vulnerability Disclosure (CVD). Available at Link to O-RAN CVD webpage.

[17] Cybersecurity and Infrastructure Security Agency (2020) "BOD 20-01: Develop and Publish a Vulnerability Disclosure Policy." Available at https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy

[18] O-RAN ALLIANCE (2026) O-RAN Security Test Specification R005-v13.00. Available at https://specifications.o-ran.org/specifications

[19] Nelson A, Rekhi S, Souppaya M, Scarfone KA (2025) Incident Response Recommendation and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-61r3. https://doi.org/10.6028/NIST.SP.800-61r3

[20] O-RAN ALLIANCE (2026) Oauth2.0 Security R005-v07.00. Available at https://specifications.o-ran.org/specifications

[21] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) NIST FIPS 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[22] Barker EB (2020) Recommendation for Key Management: Part 1 – General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 1, Rev. 5. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[23] O-RAN ALLIANCE (2026) Study on Security Configuration Management 2.0. R005-v02. Available at https://specifications.o-ran.org/specifications

[24] Cybersecurity and Infrastructure Security Agency (2026) BOD 26-04: Prioritizing Security Updates Based on Risk. Available at https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk

[25] Souppaya MP, Scarfone KA, Dodson DF (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-218. https://doi.org/10.6028/NIST.SP.800-218

Appendix A. Federal Agency Open RAN Cybersecurity Profile

Below is the O-RAN profile presented as a table for each category found in the CSF. The column descriptions are given in Section 3 with the descriptions of the first three columns matching those found in the community profile guide [3]. This profile was not intended to be used "as-is" but as a guide for federal cybersecurity managers in tailoring their own internal CSF organizational profiles. An O-RAN deployment in a federal agency could take several forms, so a single profile would not be flexible enough to meet all deployments.

A.1. CSF Governance (GV) Category

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
GV.OC-01	The organizational mission is understood and informs cybersecurity risk management	N/A	OutOfScope	O-RAN ALLIANCE Threat Analysis TR [6]	NIST SP 800-53r5 Program Management control family [7] and related controls	Low for O-RAN deployment, O-RAN is usually only a small part of an organization's infrastructure
GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	An agency's O-RAN deployment would add to an agency's risk management program.

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	N/A	OutOfScope			General USG federal agency guidance would apply, as with any system deployment
GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	N/A	OutOfScope			General USG federal agency guidance would apply, as with any system deployment
GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated	N/A	OutOfScope	O-RAN ALLIANCE specifies applications and services be described in software packages [8][9]		General USG federal agency guidance would apply, as with any system deployment
GV.RM-01	Risk management objectives are established and agreed to by organizational stakeholders	N/A	OutOfScope		Regulations/EOs around use of CSF. FISMA and NIST RMF.	

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
GV.RM-02	Risk appetite and risk tolerance statements are established, communicated, and maintained	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	General USG federal agency guidance would apply, as with any system deployment
GV.RM-03	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	General USG federal agency guidance would apply, as with any system deployment
GV.RM-04	Strategic direction that describes appropriate risk response options is established and communicated	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	General USG federal agency guidance would apply, as with any system deployment
GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	General USG federal agency guidance would apply, as with any system deployment
GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	General USG federal agency guidance would apply, as with any system deployment

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
GV.RM-07	Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	General USG federal agency guidance would apply, as with any system deployment
GV.RR-01	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	N/A	OutOfScope			General USG federal agency guidance would apply, as with any system deployment
GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	General USG federal agency guidance would apply, as with any system deployment
GV.RR-03	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	N/A	OutOfScope			General USG federal agency guidance would apply, as with any system deployment

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
GV.RR-04	Cybersecurity is included in human resources practices	N/A	OutOfScope			General USG federal agency guidance would apply, as with any system deployment
GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	N/A	OutOfScope	The O-RAN ALLIANCE has set zero trust as the target strategy for cybersecurity in Open RAN [10].	NIST SP 800-53r5 Program Management control family [7] and related controls	An O-RAN deployment would be one part of an organizational whole. Not solely a responsibility of the O-RAN admins, but instead part of the total input.
GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	An O-RAN deployment would be one part of an organizational whole. Not solely a responsibility of the O-RAN admins, but instead part of the total input.
GV.OV-01	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	General USG federal agency guidance would apply, as with any system deployment
GV.OV-02	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	General USG federal agency guidance would apply, as with any system deployment

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
GV.OV-03	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	N/A	OutOfScope		NIST SP 800-53r5 Program Management control family [7] and related controls	General USG federal agency guidance would apply, as with any system deployment
GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	N/A	OutOfScope	O-RAN ALLIANCE has requirements on including SBOMs in software packages that can aid in supply chain management [11].	General USG federal agency guidance would apply, as with any system deployment. See NIST SP 800-18 Rev 2 for more information [12].	

A.2. CSF Identify (ID) Category

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
ID.AM-01	Inventories of hardware managed by the organization are maintained	HIGH	MED	O-RAN ALLIANCE WG11 identifies rogue O-RUs as a threat [6]	BoD 23-01 on networked assets [13]	

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained	HIGH	HIGH (Rogue O-RUs) MED/LOW (other)	O-RAN ALLIANCE security requirements around SBOMs in software packages [11]	BoD 23-01 on networked assets [13]	
ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained	MED	MED	O-RAN ALLIANCE WG11 Security Continuous Monitoring TR discusses risks if data flows are not identified/monitored [14].		
ID.AM-04	Inventories of services provided by suppliers are maintained	MED	OutOfScope			Existing Policies around maintaining asset and service inventory would apply. O-RAN allows for external services and data to be accessed by O-RAN elements to enrich RAN policies.
ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission	HIGH	OutOfScope, only collection of information is required, no requirement on use	O-RAN ALLIANCE WG11 Threat Analysis report may help in the ranking [6]		

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained	HIGH	HIGH	O-RAN ALLIANCE defines relevant data types used for RAN management that may fall under this outcome.		
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	HIGH	HIGH (threats on subverted architectural elements/NFs/ rApps/xApps)	O-RAN ALLIANCE security requirements around SBOMs in software packages [11]	Agency policies would apply, NIST 800-37 Rev 2 offers guidance [15]. USG security controls in NIST SP 800-53r3 [7] on media sanitation and destruction are more stringent than O-RAN ALLIANCE controls [11].	
ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	HIGH	HIGH (O-Cloud, apps), MED (O-RU)	O-RAN ALLIANCE security requirements include requirement that vendors identify known vulnerabilities in O-RAN software [11]		
ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	MED	OutOfScope	O-RAN ALLIANCE SBOM requirements may aid in triage of new threats involving vulnerabilities to software package [11].	NIST SP 800-53r5 has control on establishing a threat awareness program (PM-16) [7]	
ID.RA-03	Internal and external threats to the organization are identified and recorded	MED	HIGH	O-RAN ALLIANCE Threat Analysis Report lists threats to O-RAN [6]		O-RAN deployment threats would need to be integrated into agency wide threat analysis.

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	HIGH	HIGH (O-Cloud, apps), MED (O-RU)	O-RAN ALLIANCE Threat Analysis Report lists threats to O-RAN [6]		
ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	MED	OutOfScope	O-RAN ALLIANCE Threat Analysis Report lists threats to O-RAN [6]	NIST SP 800-53r5 PM and Risk Assessment (RA) families [7].	
ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated	MED	OutOfScope			O-RAN deployment would need to be integrated into agency wide risk management program.
ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	MED	OutOfScope	O-RAN ALLIANCE WG11 has security requirements on logging configuration changes [11].	O-RAN logging would have to be configured according to NIST SP 800-53r5 Configuration Management (CM) controls [7]	

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
ID.RA-08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	HIGH	OutOfScope, O-RAN ALLIANCE has requirements around vuln disclosure, but not on its use	O-RAN ALLIANCE Coordinated Vulnerability Disclosure (CVD) webpage [16]	Agencies may need to have a process where vulnerabilities to their O-RAN deployment reported via their BoD 20-01 process [17] are forwarded to the O-RAN ALLIANCE.	
ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	N/A	HIGH (threats on subverted architectural elements/NFs/ rApps/xApps)	O-RAN ALLIANCE has security requirements around the integrity protection of software packages [11].		
ID.RA-10	Critical suppliers are assessed prior to acquisition	N/A	OutOfScope			Normal agency policies would apply to O-RAN component supplies. Agencies would need to check O-RAN components using the Supply Chain Risk Management (SR) family of controls in NIST SP 800-53r5 [7]
ID.IM-01	Improvements are identified from evaluations	MED	OutOfScope		NIST SP 800-53 has controls about using Pen-test/Red Teaming to find vulnerabilities that may apply to O-RAN deployment [7].	

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	MED	OutOfScope	O-RAN ALLIANCE security testing is done under Global System for Mobile Association (GSMA) Network Equipment Security Assurance Scheme (NESAS) authority based on O-RAN ALLIANCE defined test procedures [18].		
ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities	LOW	OutOfScope			
ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	N/A	OutOfScope		NIST 800-61r3 contains guidance on incident response plans and risk management [19]. NIST SP 800-53r5 has control family on incident response that would also apply [7].	

A.3. CSF Protect (PR) Category

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	HIGH	HIGH	O-RAN ALLIANCE security requirements include requiring a unique ID and X.509 credentials for every O-RAN architectural element [11].	Agencies may wish to integrate existing process identities for O-RAN to address NIST SP 800-53r5 controls [7].	
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	N/A	MED - threats of spoofing, but creds to tied to context, only per element	O-RAN ALLIANCE primarily relies on X.509 certificates for workload credentials [11].		
PR.AA-03	Users, services, and hardware are authenticated	HIGH	HIGH (RUs & unauthenticated xApps/rApps)	O-RAN ALLIANCE mandates services and architecture elements must use mTLS for authentication [11]	Agencies may wish to integrate existing process identities for O-RAN to address NIST SP 800-53r5 Access Control family [7].	
PR.AA-04	Identity assertions are protected, conveyed, and verified	MED	MED/HIGH, depending on asset (O-RU is HIGH,	O-RAN ALLIANCE requires X.509 certificates for workloads, and recommends certificates for administrators instead of password based solutions [11].	Agencies may wish to integrate existing process identities for O-RAN to address NIST SP 800-53r5 Access Control family [7].	
PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	HIGH	HIGH	O-RAN ALLIANCE includes requirements for using Oauth2 tokens [20] for authorization and requires policies set with least privilege [11].	Agencies will need to establish Oauth2 policies for O-RAN to address NIST SP 800-53r5 Access Control family [7].	

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk	N/A	MED (physical access to O-RUs)	O-RAN ALLIANCE security requirements against physical attacks against servers used for O-Cloud [11]	NIST SP 800-53r5 Physical and Environmental Protection (PE) control family [7] may override O-RAN security requirements.	
PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	MED	OutOfScope		Agency may wish to include O-RAN into training required to meet NIST SP 800-53r5 Awareness and Training (AT) controls [7].	
PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	MED	OutOfScope		Agency may wish to include O-RAN into training required to meet NIST SP 800-53r5 Awareness and Training (AT) controls [7].	
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	HIGH	HIGH (NearRT-RIC)	O-RAN ALLIANCE security requirements for DoS resistance [11].	Agencies must ensure cryptographic modules used are FIPS 140-3 approved [21] and should follow guidance on key management in NIST SP 800-57pt1 [22]	
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	HIGH	HIGH (NearRT-RIC), LOW (O-FH)	O-RAN ALLIANCE security requirements on TLS for confidentiality and requirements for DoS resistance [11].	Agencies must ensure cryptographic modules used are FIPS 140-3 approved [21] and should follow guidance on key management in NIST SP 800-57pt1 [22]	

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	MED	OutOfScope		Agencies must ensure cryptographic modules used are FIPS 140-3 approved [21] and should follow guidance on key management in NIST SP 800-57pt1 [22]	
PR.DS.11	Backups of data are created, protected, maintained, and tested	MED	HIGH	O-RAN ALLIANCE security requirements on protecting backups for O-Cloud and for security logs [11].	NIST SP 800-53r5 has controls around entire system backups [7] which do not appear in O-RAN ALLIANCE requirements	
PR.PS-01	Configuration management practices are established and applied	MED	HIGH (for O-RU, xApps, rApps)	O-RAN ALLIANCE Report on Security Configuration Management [23].	Agencies should make sure O-RAN configuration mechanism comply with applicable NIST SP 800-53r5 Configuration Management (CM) family controls [7].	
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	HIGH	O-RAN Supply chain threats	O-RAN ALLIANCE has security requirements on protecting the integrity of updates [11], but does not require updates	Agencies should integrate O-RAN components into their software maintenance plan according to CISA BoD 26-04 [24]	
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	LOW	O-RAN Supply chain threats		Agencies should integrate O-RAN components into their hardware maintenance plan according to CISA BoD 26-04 [24]	
PR.PS-04	Log records are generated and made available for continuous monitoring	HIGH	HIGH	O-RAN ALLIANCE security requirements on logging of security events [11].	Agencies should integrate O-RAN logging into agency continuous monitoring policies to meet NIST SP 800-53r5 Assessment, Authorization and Monitoring (CA) family controls [7].	

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
PR.PS-05	Installation and execution of unauthorized software are prevented	MED	HIGH	O-RAN ALLIANCE Threat Analysis [6] mainly focuses on unauthorized access/modification of O-RAN components.		
PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	LOW	OutOfScope		Agencies should ensure use of the Secure Software Development Framework (NIST SP 800-218) [25] for software applications as required.	
PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	HIGH	HIGH	O-RAN ALLIANCE security requirements on strict authentication and authorization between O-RAN components and in administration [11]	Agencies may wish to integrate existing process identities for O-RAN to address NIST SP 800-53r5 Access Control family [7].	
PR.IR-02	The organization's technology assets are protected from environmental threats	LOW	OutOfScope	N/A	NIST SP 800-53r5 Physical and Environmental Protection (PE) control family [7].	
PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	MED	HIGH (DoS threats)	O-RAN ALLIANCE security requirements that apps and network functions be able to recover from volumetric DoS attacks [11].	Agencies also need to include controls found in NIST SP 800-53r5 dealing with resilience, contingency plans and DoS protection, which go into more detail than O-RAN ALLIANCE security requirements [7].	

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
PR.IR-04	Adequate resource capacity to ensure availability is maintained	MED	HIGH (DoS threats)	O-RAN ALLIANCE security requirements that apps and network functions be able to recover from volumetric DoS attacks [11].	Agencies also need to include controls found in NIST SP 800-53r5 dealing with resilience, contingency plans and DoS protection, which go into more detail than O-RAN ALLIANCE security requirements [7].	

A.4. CSF Detect (DE) Category

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
DE.CM-01	Networks and network services are monitored to find potentially adverse events	HIGH	MED	O-RAN ALLIANCE security requirements on logging of security related events [11].	Agencies should integrate O-RAN element logs into monitoring controls in NIST SP 800-53r5 [7].	
DE.CM-02	The physical environment is monitored to find potentially adverse events	N/A	MED/HIGH (O-RU connections to O-DU)		NIST SP 800-53r5 Physical and Environmental Protection (PE) control family [7].	
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	MED	Out of Scope	O-RAN ALLIANCE security requirements on logging of security related events, but only for O-RAN elements [11].	Agencies should integrate O-RAN logs into solutions used to meet the Access Control (AC) and Supply Chain Risk Management (SR) family controls in NIST SP 800-53r3 [7].	May vary based on the data protection and risk for the given O-RAN deployment.

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	MED	HIGH (PTP in fronthaul), MED (other)	O-RAN ALLIANCE security requirements on logging of security related events, but only for O-RAN elements [11].	Agencies should integrate O-RAN logs into solutions used to meet the Access Control (AC) family controls in NIST SP 800-53r3 [7].	
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	HIGH	MED	O-RAN ALLIANCE security requirements on logging of security related events, but only for O-RAN elements [11].	Agencies should integrate O-RAN logs into solutions used to meet the controls in NIST SP 800-53r3 [7].	
DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	MED	OutOfScope		Agencies should apply relevant controls in the Risk Assessment (RA) family of controls in NIST SP 800-53r5 [7]	
DE.AE-03	Information is correlated from multiple sources	MED	MED	O-RAN ALLIANCE requirements for every architecture element to send logs to a centralized log collector [11]	Agencies should include O-RAN component logs into existing monitoring frameworks used to meet controls in NIST SP 800-53r5 [7]	
DE.AE-04	The estimated impact and scope of adverse events are understood	MED	OutOfScope		Agencies should apply relevant controls in the Risk Assessment (RA) family of controls in NIST SP 800-53r5 [7]	
DE.AE-06	Information on adverse events is provided to authorized staff and tools	MED	OutOfScope		Agencies should apply relevant controls in the Risk Assessment (RA) family of controls in NIST SP 800-53r5 [7]	Agency wide policies would apply, not just for O-RAN deployments.

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis	MED	OutOfScope		Agencies should integrate O-RAN into any existing threat intelligence system set up to meet Program Management (PM) or Risk Assessment (RA) family of controls in NIST SP 800-53r5 [7].	
DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	Potentially HIGH, based on regional laws/regulations	OutOfScope	O-RAN ALLIANCE requirements for logging that may signal incident, but no specific requirements on how they should be used.	Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	

A.5. CSF Respond (RS) Category

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	MED	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	

RS.MA-02	Incident reports are triaged and validated	HIGH	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	
RS.MA-03	Incidents are categorized and prioritized	HIGH	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	
RS.MA-04	Incidents are escalated or elevated as needed	N/A	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	
RS.MA-05	The criteria for initiating incident recovery are applied	MED	OutOfScope	O-RAN ALLIANCE security requirements include security logs and monitoring, which may be critical for measuring baseline operations [11]	Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	
RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident	MED	OutOfScope	O-RAN ALLIANCE security requirements include security logs and monitoring [11], which may be critical for measuring baseline operations and in investigations	Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	

RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	MED		O-RAN ALLIANCE security requirements include integrity protection of log data [11]	Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	
RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved	HIGH		O-RAN ALLIANCE security requirements include integrity protection of log data [11]	Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	
RS.AN-08	An incident's magnitude is estimated and validated	LOW	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	
RS.CO-02	Internal and external stakeholders are notified of incidents	HIGH: This may have additional requirements to report to regulators or law enforcement depending on relevant laws/regulations	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. NIST SP 800-53r5 also has controls around notification policies with stakeholders. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	
RS.CO-03	Information is shared with designated internal and external stakeholders	MED/HIGH: This may have additional requirements to report to regulators or law enforcement depending on relevant laws/regulations	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. NIST SP 800-53r5 also has controls around notification policies with stakeholders. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	

RS.MI-01	Incidents are contained	HIGH	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [16]. Agencies may also consider guidance in NIST SP 800-61r3 [20] on incident response.	
RS.MI-02	Incidents are eradicated	MED	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	

A.6. CSF Recover (RC) Category

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process	MED	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	
RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed	N/A	OutOfScope		NIST SP 800-53r5 has the Program Management (PM) control family that include recovery plans [7]	

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration	MED	MED	O-RAN ALLIANCE security requirements that some backups must have integrity protection [11]	Agencies need to use cryptographic modules approved for Federal use for backup integrity protection. NIST SP 800-53r5 has controls around backups of relevant operational information [7].	
RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	MED	OutOfScope		Agencies may need to set up a policy around incident response and recovery according to the Incident Response (IR) family in NIST SP 800-53r5 [7].	
RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	HIGH	HIGH (Supply Chain & DoS)	O-RAN ALLIANCE security requirements that network interfaces be able to recover/return to normal service levels after DoS attacks [11]. Out of Scope otherwise.	NIST SP 800-53r5 has controls on the create, maintaining and utilizing plans and backups to restore system components [7]. Agencies should include O-RAN components into these plans.	
RC.RP-06	The end of incident recovery is declared based on criteria, and incident related documentation is completed	LOW	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	

CSF Identifier	Outcome	Priority	O-RAN Threat Analysis TR Risk Score (Rationale)	O-RAN ALLIANCE TS/TR that Support Outcome	Other Guidance that may Support Outcome	Notes
RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	HIGH - this might be influenced by any laws/regulations regarding disclosure of incidents to regulators and/or law enforcement	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. NIST SP 800-53r5 also has controls around notification policies with stakeholders. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	
RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging	MED	OutOfScope		Agencies may need to set up a policy around incident response according to the Incident Response (IR) family in NIST SP 800-53r5 [7]. NIST SP 800-53r5 also has controls around notification policies with stakeholders. Agencies may also consider guidance in NIST SP 800-61r3 [19] on incident response.	