Defense Industrial Base (DIB) Guide to Implementing the Cybersecurity Framework

OCTOBER 4, 2019

CLEARED
For Open Publication

Oct 15, 2019 5

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Foreword

The National Institute of Standards and Technology (NIST) released the *Framework for Improving Critical Infrastructure Cybersecurity* ("Framework") as a voluntary, risk-based set of standards and best practices to help organizations of all sizes manage cybersecurity risks in any sector.

As the Sector Specific Agency for the Defense Industrial Base (DIB), DoD has adopted a multipronged approach that includes both mandatory and voluntary cybersecurity activities with the DIB. The voluntary DIB Cybersecurity (CS) Program offers cleared defense contractors a collaborative cyber threat sharing environment. From a contractual standpoint, under Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.202-7102, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, DoD contractors are required to report cyber incidents, as well as implement the security requirements in NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

This *Defense Industrial Base Guide to Implementing the Cybersecurity Framework* ("Guide"), supports DoD's critical infrastructure responsibilities for the DIB. This Guide was developed working with our private sector partners to implement the Framework, while also incorporating the security requirements of NIST SP 800-171. The Guide is intended as a resource that organizations can use to manage their cybersecurity program and meet the requirements of the DFARS. As a companion document, the *DIB Guide Template for Implementing the Cybersecurity Framework* ("Template") can be used by organizations as a management tool to assist in implementing the seven-step process outlined in the Framework. Throughout the Guide, illustrative references are made to the Template. The fields on the Template correspond to the seven-step process in the Framework. Given the amount of fields on the Template and its granularity presenting all 108 Subcategories, the Template is not easily printed and is designed as an online tool.

This Guide and supporting online Template are intended to assist an organization in evaluating current and desired cybersecurity outcomes that support a more comprehensive approach to cybersecurity. Organizations can use this Guide as a roadmap for achieving a desired state of cybersecurity risk management practices and assess how their current activities align with DoD requirements.

This Guide and Template are applicable to all organizations in the DIB — regardless of their size, cybersecurity risk, or current level of cybersecurity sophistication. The Framework and this Guide are focused on helping individual organizations reduce and better manage their cybersecurity risks, contributing to a more secure and resilient sector overall.

This Guide is built around the primary functional areas ("Functions") of the Framework (i.e., Identify, Protect, Detect, Respond, and Recover), which encompass the full spectrum of cybersecurity activities, and the seven-step implementation process presented in the Framework.

DoD would like to recognize the contributions in drafting this document made by the Department of Homeland Security's 2015 *Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance*, NIST's 2017 *Cybersecurity Framework Manufacturing Profile* and 2016 *Small Business Information: The Fundamental*s. This Guide also incorporates the latest changes from the Cybersecurity Framework V1.1 released in April 2018.

Table of Contents

Foreword **1**

Introduction **3**

Cybersecurity Framework Guide Overview and Benefits **4**
- Potential Benefits of Implementing the Cybersecurity Framework 4

Cybersecurity Framework Structure **4**
- Cybersecurity Framework Core 4
- Implementation Tiers 7
- Cybersecurity Framework Profile 8

Framework Implementation **8**
- Step 1: Prioritize and Scope 10
- Step 2: Orient 10
- Step 3: Create a Current Profile 11
- Step 4: Conduct a Risk Assessment 12
- Step 5: Create a Target Profile 12
- Step 6: Determine, Analyze, and Prioritize Gaps 13
- Step 7: Implement Action Plan 14

Conclusion **15**

Appendix A: Tools and Resources **16**

Appendix B: Framework Implementation Tiers **17**
- Tier 1: Partial 17
- Tier 2: Risk Informed 17
- Tier 3: Repeatable 18
- Tier 4: Adaptive 18

Introduction

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, directed the development of a voluntary cybersecurity framework. The Executive Order charged NIST to develop the *Framework for Improving Critical Infrastructure* to provide a common language that critical infrastructure organizations can use to assess and manage their cybersecurity risk.

The Framework is designed to complement an organization's risk management process and cybersecurity program. The Framework broadly applies across all organizations, regardless of size, industry, or cybersecurity sophistication.

The Framework can help guide an organization in improving cybersecurity and thereby improve the security and resilience of critical infrastructure. The Framework applies whether an organization has a mature risk management program and processes, is developing a program or processes, or has no program or processes.

This Guide facilitates the application of the Framework to the DIB. It highlights the linkages between implementing the Framework and implementing the security requirements in NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.*

This Guide is intended to be used in conjunction with the companion Template. The Template provides an organized construct for applying the Framework by assisting an organization in evaluating their cybersecurity Current Profile(s), determining their Target Profile(s), identifying gaps and implementing an action plan.

This Guide and Template support organizations with implementing the seven steps for establishing or improving a cybersecurity program described in the Framework. This structured process of assessing Current Profiles and determining Target Profiles will assist organizations in preparing a System Security Plan as they identify how security requirements are being met including those identified by DoD. As security requirements evolve, this framework will enable the DIB to address new cyber threats in a structured and responsive process.

Cybersecurity Framework Guide Overview and Benefits

The Framework was developed based on input from multiple critical industry sectors and includes a collection of related cybersecurity standards and industry best practices. The Framework:

- Provides guidance on risk management principles and best practices;
- Provides a common language to address and manage cybersecurity risk;
- Outlines a structure for organizations to understand and apply cybersecurity risk management; and
- Identifies effective standards, guidelines, and practices to manage cybersecurity risk in a cost-effective manner.

The Framework broadly applies across all organizations, regardless of size, industry, or cybersecurity sophistication. The Framework can help guide an organization in improving cybersecurity and thereby improve the security and resilience of critical infrastructure.

For those DIB organizations charged with implementing the security requirements outlined in NIST SP 800-171, this Guide highlights the linkages between implementing the Framework and accomplishing the NIST SP 800-171 security requirements.

Potential Benefits of Implementing the Cybersecurity Framework

Choosing to implement the Framework means that the organization wishes to take advantage of the benefits that the Framework offers and does not imply that an existing cybersecurity and risk management approach is ineffective or needs to be replaced. Specifically, implementing the Framework provides a mechanism for an organization to:

- Assess and specifically **describe its current and targeted cybersecurity posture**.
- **Identify gaps** in its current programs and processes.
- Identify and **prioritize opportunities for improvement** using a continuous and repeatable process.
- **Assess progress** toward reaching its target cybersecurity posture.
- **Communicate cybersecurity posture in a common, recognized language** to internal and external stakeholders—including customers, regulators, investors, and policymakers.

Cybersecurity Framework Structure

The Framework uses three main components—Core, Implementation Tiers, and Profiles—which enable an organization to identify its cybersecurity practices, provide context for its cybersecurity approach, and describe its current and target (or goal) cybersecurity posture. These three components help an organization examine its cybersecurity activities in terms of its specific priorities.

Cybersecurity Framework Core

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes with reference guidance to achieve these outcomes. The Core comprises of four elements: Functions, Categories, Subcategories and Informative references.

1. **Functions:** The Core Functions organize cybersecurity activities at the highest level and enable an organization to focus their attention on developing a strategic view of their cybersecurity postures. Although the Functions do not replace a risk management process, they provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk, so they can assess how identified risks are managed and to see how their organizations align with existing cybersecurity standards, guidelines, and practices. The five "functions" of the Framework Core are:

    a) *Identify* – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

    b) *Protect* – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

    c) *Detect* – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

    d) *Respond* – Develop and implement the appropriate activities to act regarding a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

    e) *Recover* – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

2. **Categories:** Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and activities. In the Identify Function, for example, Categories include Asset Management, Business Environment, Governance, Asset Management, Risk Assessment and Risk Management Strategy.

TABLE 1. CYBERSECURITY FRAMEWORK FUNCTIONS AND CATEGORIES

Function Unique Identifier	Function	Category Unique Identifier	Category
		ID.AM	Asset Management

ID	Identify	ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

3. **Subcategories:** Subcategories are the subcomponents of Categories and detail the specific outcomes of the activity, tool, or approach used in the category. While not exhaustive, Subcategories help support achievement of the outcomes in each Category. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated. The organization implements these Subcategories, and any other activities necessary, to address the risk in their organization's environment.

4. **Informative References:** The Informative References point to examples of specific sections of standards, guidelines, and practices that help organizations achieve the outcomes associated with each Subcategory. The Informative References are based on cross-sector guidance and are not exhaustive. NIST encourages organizations to enhance the Informative References with any additional applicable resources, such as industry-specific standards and internal practices.

   The security requirements in NIST SP 800-171 have been mapped to the Subcategories as additional Informative References. These requirements provide a minimum cybersecurity baseline to protect DoD controlled unclassified information (CUI) residing or transiting DIB internal networks or information systems.

Some NIST SP 800-171 requirements do not map to any Framework Subcategories because NIST SP 800-171 focuses solely on protecting the confidentiality of CUI in non-federal systems. The expectation is that organizations will also use other industry standards and best practices in developing a comprehensive cybersecurity program.

In addition, for organizations in the DIB that use a cloud service provider, DoD CUI must be protected at the FedRAMP moderate level based on the moderate security control baseline in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.* The Informative References section on the Template maps the Framework Subcategories to NIST 800-53 Rev 4 controls.

The activities described in Subcategories can be performed concurrently and continuously to form an operational construct that addresses the dynamic cybersecurity risk. As shown in Table 2, the Informative References provide examples of standards and guidelines that can be used to implement each Subcategory. The relevant requirements from NIST SP 800-171 and the moderate controls from NIST SP 800-53 are listed for the Subcategory "Physical devices and systems within the organization are inventoried."

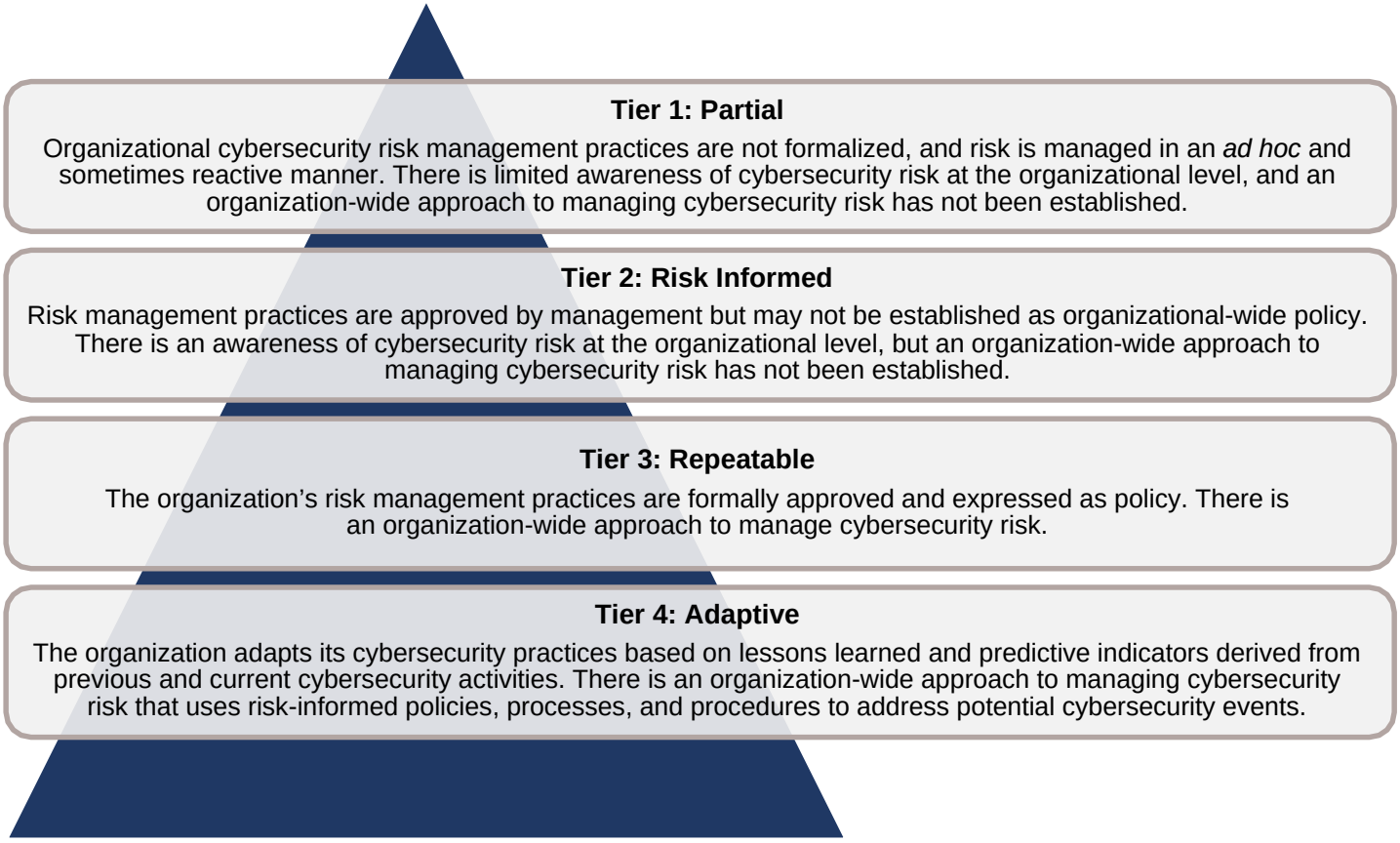
TABLE 2. FRAMEWORK CORE STRUCTURE

Functions	Categories	Subcategories	Informative References
Organize **basic cybersecurity activities** at their highest level and align with existing methodologies for incident management.	Subdivide Functions into groups of particular **cybersecurity activities** or programmatic **needs**.	Divide further into **specific outcomes** of technical and management activities. **Expressed as *results*.**	Reference specific sections of standards, guidelines, and practices that **illustrate a method to achieve the outcomes** of each Subcategory.
IDENTIFY	**Asset Management**	ID.AM-1: Physical devices and systems within the organization are inventoried	-NIST SP 800-171 Rev. 1 3.4.1 -NIST SP 800-53 Rev. 4 CM-8 -CCS CSC 1 -COBIT 5 BAI09.01, BAI09.02 -ISA 62443-2-1:2009 4.2.3.4 -ISA 62443-3-3:2013 SR 7.8 -ISO/IEC 27001:2013 A.8.1.1, A.8.1.2

Implementation Tiers

The Framework presents Implementation Tiers to outline how an organization views and handles cybersecurity risk and the processes in place to handle that risk. The Tier selection process considers an organization's risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business objectives and organizational constraints. The Tiers help assess progress in managing and evaluating a cybersecurity program over time. An objective target for the DIB should be Tier 3 in which the organization's risk management practices are formally approved and expressed as policy and there is an organization-wide approach to manage cybersecurity risk. This Guide focuses on the near term effort of implementing the Core Elements through the seven-step process of assessing Current Profiles and determining Target Profiles. Over time, this process will impact an organization's Tier status, but it is not the focus of this Guide. More discussion on Tiers is presented at Appendix B.

FIGURE 1. FRAMEWORK TIERS



Cybersecurity Framework Profile

A Framework Profile aligns business requirements, risk tolerance, and resources of the organization to the Core Elements and establishes an organization's cybersecurity state. A Profile can represent an organization's current cybersecurity posture ("Current Profile") or its target cybersecurity state ("Target Profile"). Organizations can compare their Current and Target Profiles as part of their strategic planning process to identify gaps and activities to reach that end state. Ultimately, Profiles provide a mechanism to reduce cybersecurity risk with outcomes based on an organization's mission and business needs. This Guide will provide further instructions on how an organization can develop its Current and Target Profile.

Framework Implementation

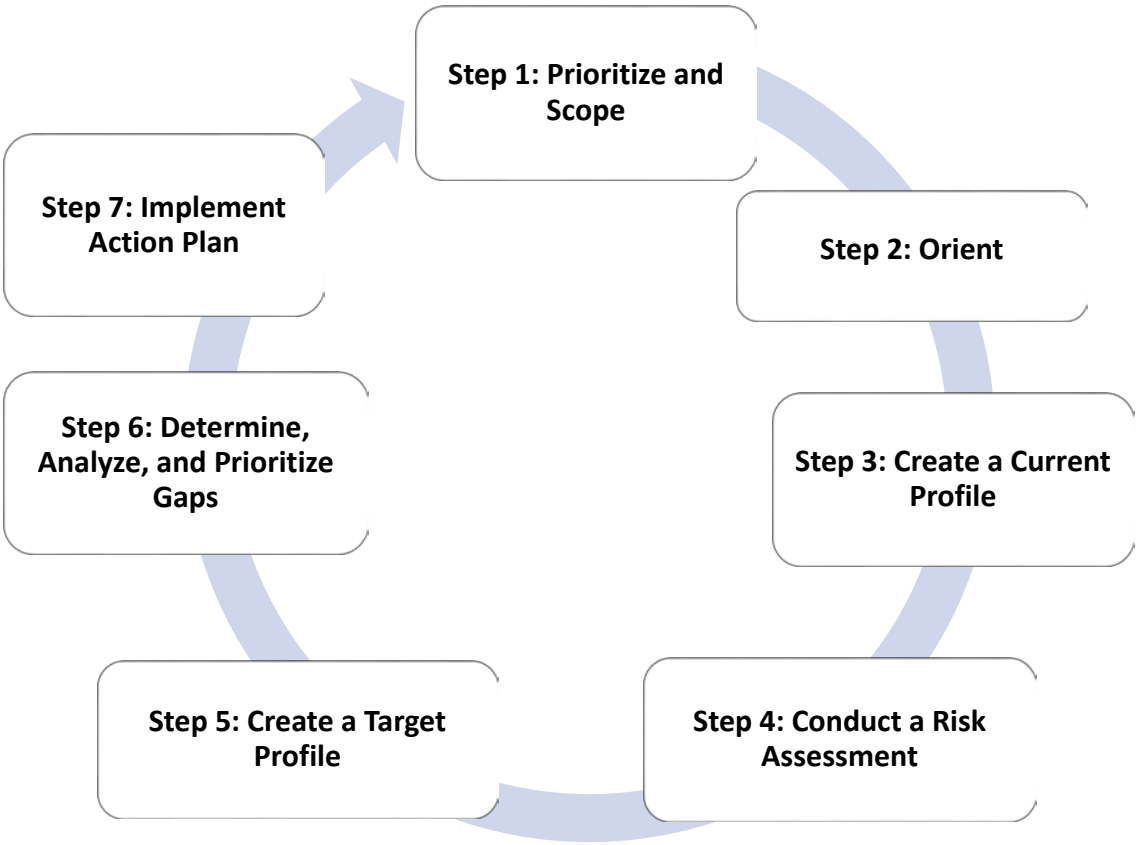
Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and priority expenditures to maximize the impact of the investment. The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a tool for improving an existing program. It can also help identify gaps in an organization's cybersecurity practices.

How organizations implement the Framework depends on multiple factors, including whether the organization has already established a cybersecurity program, the risk posture of the organization, and available resources. An organization can use the Framework as a key part of its systemic process for identifying, assessing, and managing

cybersecurity risk. Implementing the Framework includes mapping current risk management activities, programs, and tools to the Framework Core, prioritizing activities in the Core and aligning them to mission and business objectives to create one or more Target Profiles, and evaluating current and desired Implementation Tiers.[1] Once gaps and differing needs are understood, the organization can begin identifying approaches and resources to address them. This Guide provides further information for using the Framework within the DIB community.

For those organizations seeking to actively use the Framework to build a cybersecurity risk management program, the Framework presents a seven-step process for implementation. An organization can use this approach with any cybersecurity standard or tool for managing cybersecurity risk. The seven-step process is shown in Figure 2. The approach can be an iterative process repeated to address the evolving risk environment.

FIGURE 2. IMPLEMENTATION STEPS AND KEY



[1] Applicable industry-focused Framework Profiles can be used to accelerate this process. Although industry-focused Profiles are not explicitly discussed in the Cybersecurity Framework, they are an emerging practice in multiple industries. NIST shares several examples in the References section of its Cybersecurity Framework website (available at: https://www.nist.gov/cyberframework). Industry-focused Profiles are effectively a Target Profile for the organizations within their context. For example, the U.S. Coast Guard developed an Offshore Operations Cybersecurity Framework Profile that oil and natural gas companies that perform offshore drilling and production activities use to inform development of their individual Target Profiles.

Step 1: Prioritize and Scope

When implementing the Framework, an organization first identifies its business or mission objectives and its strategic priorities as they relate to cybersecurity. With this information, an organization can make decisions regarding cybersecurity implementation and determine the breadth and scope of systems and assets that support its objectives.

The following overarching strategic objectives, developed in coordination with input from industry participants in the voluntary DIB CS program, are provided for consideration by organizations:

- **Maintain Stability:** The DIB organization preserves operational stability such that processes and systems continuously underpin production and service goals with the objective of supporting profitability and reputation.

- **Create Value for Stakeholders:** The DIB organization's activities facilitate and promote achievement of its mission and provide an effective environment for future development which create value added for an organization's stakeholders, both internal and external, including DoD elements they support.

- **Preserve Business Operations and Continuity:** The DIB organization implements resiliency practices that support its on-going ability to execute its current and future lines of operation.

- **Protect Controlled and Sensitive Information:** The DIB organization manages risks to the intellectual property and sensitive business and Government data that it maintains.

These objectives are not focused exclusively on cybersecurity, as cybersecurity serves as an enabler supporting these overarching objectives. These business/mission objectives provide the initial context for identifying and managing applicable cybersecurity risk mitigation pursuits. Each DIB organization should supplement these objectives with others that are relevant its operations. The objectives mark the starting point for identifying enabling cybersecurity practices, which allows organizations to better prioritize actions and resources according to the organizations' defined needs.

Current threat and vulnerability information (e.g., information from important vendors, communication of threats to the DIB from the DIB CS program, or other threat advisories) may also help inform cybersecurity program decisions. Cyber threats to the DIB are increasing and organizations must address the threat to protect their sensitive and proprietary business information.

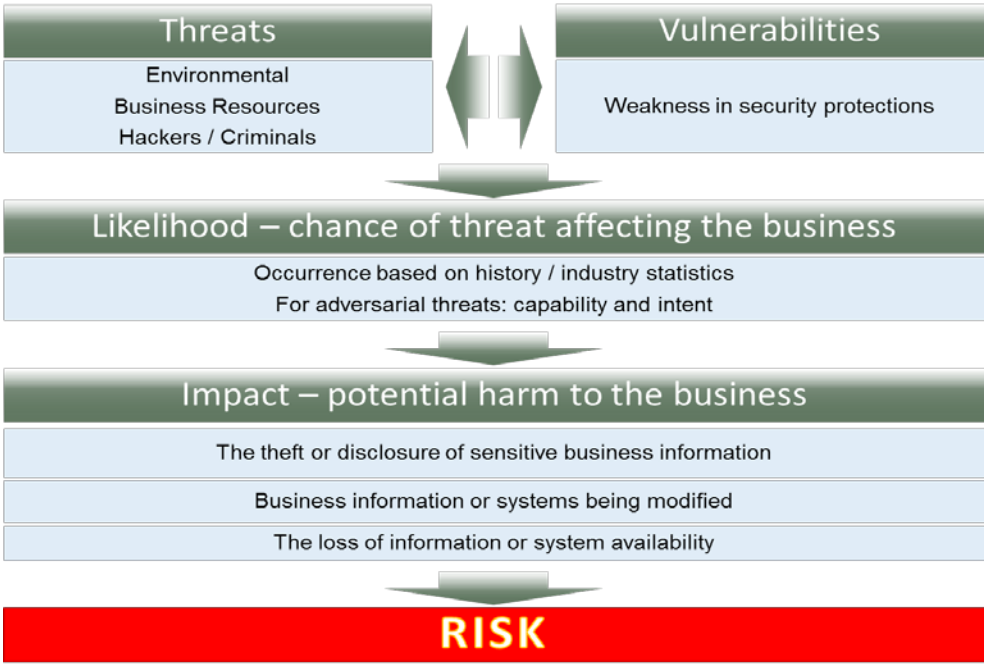
To gain familiarity and experience, an organization using the Framework for the first time may apply it to a small subset of operations. For example, an organization may choose to begin with business functions that are already undergoing similar or related risk management efforts or a moderate risk mission function with known or suspected gaps. Then, with a greater understanding, the organization can apply the Framework to a broader subset of operations or to additional divisions of the organization.

Step 2: Orient

Once the scope of the cybersecurity program has been determined, an organization identifies the systems, assets, requirements, and risk management approaches that fall within the scope of the effort. This includes current organization standards and best practices, as well as any additional items that can enable the organization to achieve its critical infrastructure mission and business objectives for cybersecurity risk management.

As shown in Figure 3, risk is a function of threats, vulnerabilities, the likelihood of an event, and the potential impact such an event would have to the organization. By understanding risks in the context of objectives, an organization can know where to focus their efforts. While eliminating all risks is an unlikely goal, a realistic goal is to provide reasonable assurance that informed decisions are made regarding the management of cybersecurity risks.

FIGURE 3. RELATIONSHIP BETWEEN THREATS, VULNERABILITIES, IMPACT, & LIKELIHOOD



In general, organizations should focus initially on critical systems and assets and then expand into systems and assets that are less critical or central to their mission and business objectives.

Organizations can use a variety of methods to manage their current cybersecurity posture, including self-evaluations or facilitated approaches to identify requirements. In a self-evaluation, an organization may leverage its own resources and expertise, whereas a facilitated approach relies on the expertise of a third party. The value in a self-evaluation or a third party evaluation is the additional internal cybersecurity awareness and discovery that the activity can generate. In this regard, it is important senior executives are involved in identifying requirements that address cybersecurity risk management.

Step 3: Create a Current Profile

The Current Profile indicates the cybersecurity outcomes that are currently being achieved at the Subcategory level. The purpose of identifying a Current Profile is not only to develop a map between organizational practices, but also to help understand the extent to which such practices achieve the outcomes outlined by the Framework. The organization develops a Current Profile by indicating which Subcategory outcomes from the Framework Core are currently being achieved. To identify the Current Profile, organizations use the evaluation approach to map current cybersecurity approach and outcomes to the corresponding Subcategory outcomes in a summary statement.

System Security Plans developed in accordance with NIST SP 800-171 may inform the Current Profile. The System Security Plan documents how the organization is implementing the security requirements in NIST SP 800-171 for a system, many of which map to the Subcategories outlined in the Framework.

An organization can use the Template to document the Current Profile for their organization as a whole or for specific mission/business contexts. The Current Profile is created by identifying each Subcategory that is currently being achieved, or partially achieved.

The Template provides an example of how a mapping can be used to create a Current Profile for a specific Subcategory outcome (see ID.AM-1, column D of the Template). Note that the example in the Template is intended to be illustrative of the mapping concept and not necessarily address a specific organization's approach. The level of specificity and granularity required for Current and Target Profiles to be useful will be unique to each organization.

Step 4: Conduct a Risk Assessment

The assessment process is guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization.

It is important that the organization incorporates emerging risk, threat, and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

For organizations that already have a risk management program in place, this activity will be part of regular business practice, and necessary records and information to make this determination may already exist.

There are a variety of tools available to help organizations conduct risk assessments. NIST has developed a number of cybersecurity standards that, while not required for DIB use, may serve as valuable resources for organizations that do not have similar standards available. For example, NIST SP 800-30, *Guide for Conducting Risk Assessments*, provides guidance for conducting risk assessments for information systems and organizations. Risk assessments help organizations identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, and the Nation, resulting from the operation and use of information systems. NIST SP 800-30 provides guidance for examining risk at the organization, mission/business process, and information system levels to help decision makers make informed decisions about the risk for the organization

Step 5: Create a Target Profile

A Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management state based on the organization's mission and business objectives. Depending on the mission of the organization, some may have more than one Target Profile as business needs may vary across the enterprise. Target Profiles may address certain contexts, mission focuses or areas of complexity. While the Framework does not prescribe templates, in creating a Target Profile(s), organizations should consider:

- Current risk management practices;
- Current risk environment;
- Legal and regulatory requirements;
- Business and mission objectives; and
- Organizational constraints.

The Target Profile outlines the key Subcategory outcomes and associated cybersecurity and risk management standards, tools, methods, and guidelines that enable an organization's mission and business objectives.

It is essential the Target Profile aligns cybersecurity capabilities with mission/business needs. The Target Profile should never be just about cybersecurity objectives. Focusing the Target Profile on security objectives, without the tie to mission and business context, is one of the reasons cybersecurity programs fail to tie cybersecurity activities to specific risks or needs and struggle to prioritize cybersecurity activities.

The Profile relies on the organizations risk management process to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities.

When creating the Target Profile, the Framework gives organizations a broad overview of the cybersecurity and risk management domains, but is not all-inclusive. An organization may find it necessary to use standards, tools, methods, and guidelines that achieve outcomes not defined by the Framework. Including these practices in the organization's Target Profile(s) is also beneficial for coordination and future engagement.

The Template provides an example of a representative Target Profile for a specific Subcategory outcome (column G and column H). In Template example, the Current Profile tier rating is partial and the Target Profile tier rating is repeatable.

The alignment of the Current Profile and Target Profile will evolve as an organization's risk and operational environment changes over time. For instance, an organization may add a new mission or business objective that must be addressed by its Current and Target Profiles or determine that a current practice is no longer necessary and omit it from the Target Profile. For this reason, organizations should periodically review their Current and Target Profiles and update them as necessary.

Step 6: Determine, Analyze, and Prioritize Gaps

In this step, the organization compares the Current Profile and the Target Profile to determine gaps. This process enables the organization to make informed decisions about cybersecurity activities, supports risk management, and allows the organization to perform cost-effective, targeted improvements.

A gap exists when there is a desired Subcategory outcome in the Target Profile that is not currently satisfied by current cybersecurity and risk management approaches identified in the Current Profile, as well as situations where existing practices do not achieve the outcome required by the organization's risk management strategy.

For the DIB, developing the System Security Plan can help determine and analyze gaps on those Subcategories mapping to NIST SP 800-171.

To address gaps, the organization creates a prioritized action plan that draws on mission drivers, a cost/benefit analysis, and an understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Within the DIB, the Plans of Action and Milestones an organization develops for those security requirements not met under NIST SP 800-171 may contribute to an organization's overall prioritized action plan (step 7).

On the Template there is a column for each Subcategory to identify those gaps in more detail (column I). As noted in the example on the Template, the following gap was identified: "Need assets to be added to asset database before provisioned to employee."

Step 7: Implement Action Plan

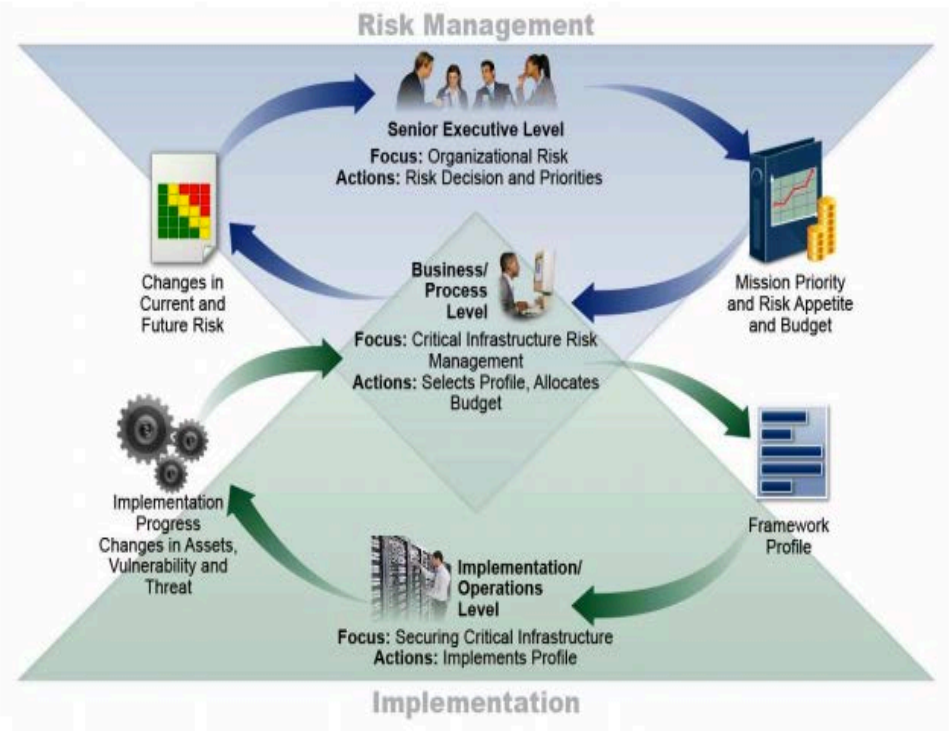
The organization determines which actions to take regarding the gaps, if any, identified in the previous step, and then monitors its current cybersecurity practices against the Target Profile.

An organization may repeat the steps as needed to continuously assess and improve its cybersecurity program. For instance, organizations may find that more frequent repetition of the Orient step improves the quality of risk assessments.

To assist organizations, Informative References are listed on the Template for each Subcategory. Additionally, the Template includes a mapping of Subcategories to NIST SP 800-171 requirements. Organizations should determine which standards, guidelines, and practices, including those that are sector-specific, work best for their needs.

In the Template, column K allows for organizations to document for each Subcategory the action plan the organization is going to take to address any identified gaps.

FIGURE 4: RISK MANAGEMENT IMPLEMENTATION



Operating cybersecurity programs requires collaboration and communication across the organization.

As outlined in Figure 4, the senior executive level communicates priorities, available resources, and overall risk tolerance. They make informed decisions based on information from the business/process level.

The business process level uses this feedback to perform an impact assessment and develop the Target Profile.

The implementation/operations level implements the Profile and communicates progress to the business/process level.

Business process level management reports the outcomes of the implementation to the executive level to shape changes in the current and future risk management process.

Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Over time, organizations may also utilize this process to align their cybersecurity program with their desired Framework Implementation Tier.

Conclusion

This Guide and the companion online Template were developed in coordination with participants in the DIB CS Program and the National Defense Information Sharing and Analysis Center. The Guide was written to apply to the wide range of organizations that comprise the DIB, from the very small to very large with varying levels of cybersecurity program maturity. This Guide will continue to be updated as policies and processes in the Department change.

Given the heightened cyber threat, the importance of a robust cybersecurity program cannot be overemphasized. Cyber threats to DIB unclassified information systems represent an unacceptable risk of compromise to both proprietary information and DoD CUI and pose an imminent threat to U.S. national and economic security interests.

Implementing the Framework facilitates cybersecurity discussions across organizations and bolsters cybersecurity. Cybersecurity must be a priority for all organizations with cybersecurity considerations integrated into organizations' business risk management processes. Cybersecurity is everyone's responsibility across an organization, from senior leaders setting priorities and allocating resources, to alert individual operators executing the organization's mission, all supported by a well-trained cybersecurity workforce.

The DoD and the DIB must work together. By leveraging the Framework, we can build capacity and strengthen safeguards with the DIB sector that will raise the bar in cybersecurity.

Appendix A: Tools and Resources

1. NIST Cybersecurity Framework
   (https://www.nist.gov/cyberframework)

2. Mapping: Cybersecurity Framework 1.0 to SP 800-171 Rev. 1
   (https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final)

3. NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1
   (https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11)

4. NIST SP 800-171, *Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations*
   (Rev. 1: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final)
   (Rev. 2: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/draft)

5. NIST SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*
   (https://csrc.nist.gov/publications/detail/sp/800-171a/final)

6. NISTR 8183, *Cybersecurity Framework Manufacturing Profile*
   (https://csrc.nist.gov/publications/detail/nistir/8183/final)

7. Department of Homeland Security, *Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance*
   (https://www.dhs.gov/publication/critical-manufacturing-cybersecurity-framework-implementation-guidance)

8. NIST MEP *Cybersecurity Manufacturing Extension Partnership, Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*
   (https://www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security)

9. *NISTIR 7621*, Revision 1, *Small Business Information Security: The Fundamentals*
   (https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final)

10. NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*
    (https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)

11. NIST Risk Management Framework
    (https://csrc.nist.gov/Projects/Risk-Management/rmf-overview)

12. NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
    (https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final)
    **The mappings to NIST SP 800-53 Rev 4 are only at the control level and the list is not exhaustive*

Appendix B: Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization's management of cybersecurity risk and potential risk responses.

The Tier definitions are as follows:

Tier 1: Partial

- *Risk Management Process* – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- *External Participation* – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

Tier 2: Risk Informed

- *Risk Management Process* – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
- *External Participation* – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated

with the products and services it provides and uses but does not act consistently or formally upon those risks.

Tier 3: Repeatable

- *Risk Management Process* – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- *Integrated Risk Management Program* – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

Tier 4: Adaptive

- *Risk Management Process* – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.
- *Integrated Risk Management Program* – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other

collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.