Transportation Systems Sector Cybersecurity Framework Implementation Guidance

Prepared June 26, 2015

Introduction

The President, under Executive Order (EO) 13636, "*Improving Critical Infrastructure Cybersecurity,*" February 2013, directed National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure, recognizing that the national and economic security of the United States depends on the reliable functioning of vital systems and assets working together to effectively manage cybersecurity dangers and liabilities. Through an open and collaborative process, NIST-engaged individuals, organizations, academia, owners and operators of critical infrastructure to develop a flexible, repeatable, and cost-effective approach, resulting in NIST's release of the voluntary Framework for Improving Critical Infrastructure Cybersecurity Framework for use across all critical infrastructure sectors on February 12, 2014. Understanding that a "one size fits all" methodology for implementation of the Framework is impractical, the Transportation Security Administration, Department of Transportation, United States Coast Guard, and Transportation Systems Sector (TSS) stakeholders organized an effort to create implementation guidance of greatest relevance to the TSS.

Purpose/Scope

The purpose of this document, TSS Cybersecurity Framework Implementation Guidance is to provide the Transportation Systems Sector guidance, resource direction, and a directory of options to assist a TSS organization in adopting the NIST Framework. The implementation guidance may be used by organizations to accomplish the following:

- Characterize their current and target cybersecurity posture.
- Identify opportunities for evolving their existing cybersecurity risk management programs..
- Recognize existing sector tools, standards, and guidelines that may support Framework implementation.
- Assess and communicate their risk management approach to both internal and external stakeholders.

This implementation guidance can be incorporated into an organization's culture regardless of the organizations current cybersecurity maturity level. For organizations that do not have a formal cybersecurity risk management program, this implementation guidance can help them to comprehend, evaluate, and establish the organizations cyber risk priorities. For those organizations that have a formal risk management office or program in place, this guidance provides additional mechanisms to review existing programs and identify areas for improvement, while aligning current efforts to the Framework.

Transportation Cyber Strategy and Framework Alignment

In 2011, as an outcome of a cybersecurity exercise involving TSS stakeholders and government partners collaborated to develop the Cybersecurity Strategy for the TSS. This document guides the Sector's efforts in managing cyber risks and improving preparedness posture through enhancing cybersecurity awareness and promoting collaborative community action. The following table shows how goals of the TSS align with sections of the Framework.

Table 1: Sector Strategy and Framework Alignment

TSS Strategy Goals	NIST Categories
Goal 1: Define Conceptual Environment	Access Control Asset Management Information Protection Processes and Procedures Maintenance Response Planning Recovery Planning Risk Management Strategy Risk Assessment
Goal 2: Improve and Expand Voluntary Participation	Communications
Goal 3: Maintain Continuous Cybersecurity Awareness	Awareness and Training Improvements Protective Technology
Goal 4: Enhance Intelligence and Security Information Sharing	Analysis Anomalies and Events Data Security Detection Processes Mitigation Security Continuous Monitoring
Goal 5: Ensure Sustained Coordination and Strategic Implementation	Business Environment Governance

The NIST Cybersecurity Framework

The Cybersecurity Framework is a risk-based approach to managing cybersecurity risk, allowing framework elements to reinforce the connection between business drivers and cybersecurity activities. The Framework was developed to complement, not replace, an organization's established risk management process and cybersecurity program. An organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. For organizations with no formal cybersecurity program in place, the Framework can provide a foundation upon which to implement a robust cybersecurity program. The Framework is composed of three parts:

- **Framework Core:** The cybersecurity activities describe desired outcomes, and references critical infrastructure sectors. The Core, broken into 5 functions, presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The functions are described as follows:
    - **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
    - **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

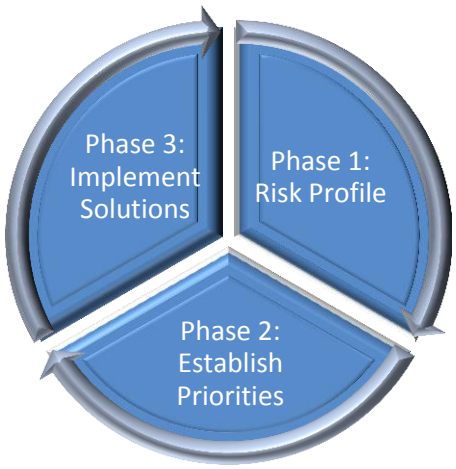
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

- **Framework Tiers:** These 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 increasing levels of effort and detail to integrate cyber risk management practices into an organization's overall risk management approach based on business need.
- **Framework Profile:** The profile represents the outcomes based on business needs, risk tolerance, and resource requirements that an organization has selected from Framework categories and subcategories. To ensure adaptability and enable technical innovation, the Framework is technology neutral. The Framework relies on a variety of existing standards, guidelines, and practices to advance critical infrastructure providers to achieve resilience.

Implementation Guidance

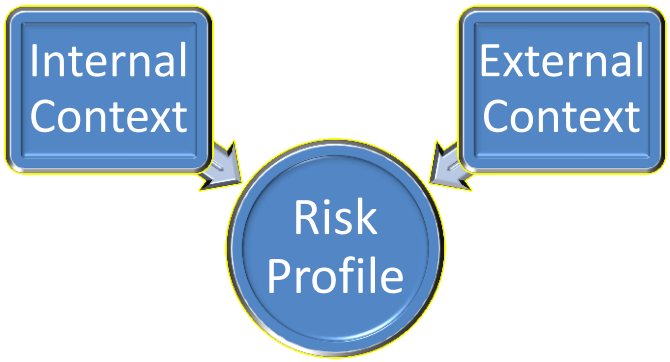
The main objective of the Implementation Guidance is to strengthen an organization's risk management approach and communicate its use of cybersecurity practices to internal and external stakeholders. As stated previously, this guidance was designed to be used by organizations of varying levels of cybersecurity and risk management maturity. The following diagram illustrates the approach that the TSS is using to assist organizations with their implementation efforts.

NIST Framework Implementation Guidance Cycle



Phase 1: Determining Risk Profile

Establishing a cyber-risk profile within an organization is the foundation of the Transportation Systems Sector's implementation of the NIST Framework. A risk profile attempts to determine the corporation's willingness to take risk (or its aversion to risk), which drives the overall decision-making strategy. It comprises two main components: internal context and external context. Assessing the internal context of the organization will show what countermeasures are in place while providing an overall snapshot of how the organization views its cybersecurity program. That combined with external context, consisting mainly of threat intelligence provided by the Department of Homeland Security and other intelligence/threat resources, will help the organization align capabilities deployed to external threats. Upon completion, the risk profile furthers an organization's understanding of its current cyber risk posture and promotes mitigation strategies to narrow the profile over a determined amount of time. Navigation of internal and external context is discussed in the sections to follow.



P1-1: Internal Context

An organization's internal context includes cultural parameters and factors that influence how risk is managed in order to achieve objectives. Understanding the internal context is fundamental to any risk management activity as it forecasts an organization's risk profile and current posture. One key element

of understanding an organization's external context is to assess its vulnerabilities. Performing a vulnerability assessment simply means identifying and reporting noted vulnerabilities and security weaknesses in an organization, which can span a broad spectrum of areas ranging from technical weaknesses within systems to the human factor based on lack of awareness. Internal assessments should be a collaborative effort between the assessment team, asset owners, and the vendor (if applicable). Involving all of these groups during the assessment process can save valuable time and ensure that all critical or insecure areas are thoroughly considered.

Identification of internal vulnerabilities is a process that involves recognizing, acknowledging, and detailing what could adversely affect the achievement of an organization's objectives. The following considerations should be taken into account prior to executing the assessment:

- The assessment team will need to carefully consider the scope of the effort and allocate resources and responsibilities accordingly.
- The assessment may require resources beyond the assessment team. Multiple components within the organization will need to support the assessment by providing data and access.
- The assessment will need to be scheduled at a time when normal operations are not in a critical or highly-stressed state in order to lessen complications or business impact.

The evaluation of internal vulnerabilities is not an extemporaneous activity. The assessment team will need to plan activities in close collaboration with operations and engineering personnel to maximize efficiency of the assessment.

Maturity Model

A maturity model is a framework used to establish targets for comparison when looking at an organization's processes. It evaluates capability and implements strategies based on level of acceptable risk. An assessment of an organization's maturity level helps determine its security posture and establish an accurate snapshot of its current cybersecurity practices, which is essential for constructing a baseline for framework implementation. Maturity models provide an internal benchmark that an organization can utilize to measure capabilities of structural practices, assess processes and methods currently implemented, establish allocation of resources, and establish goals and priorities for enhancements. When used correctly, maturity models create a snapshot of an organization's present cybersecurity posture and identify areas of opportunity for enhancement.

Another benefit of completing a maturity model is that it enables an organization to assess its capabilities in relation to, and establish a crosswalk document that maps the maturity levels to, the Framework. When selecting an approach, the organization should evaluate capabilities applicable to its mission and objectives. Ultimately, it is up to the individual organization to determine which of the models and practices are most relevant. Appendix 1 lists common maturity models currently utilized within organizations that the TSS recognizes for adoption of the Framework.

P1-2: External Context

Trend analysis is an integral component of performing a comprehensive examination of an organization's risk profile. Combining the practice of collecting information and attempting to spot a

pattern, or trend, within that information with a maturity model will drive an organization's ability to prioritize initiatives. A valid trend analysis can identify priorities upon receiving an organization's valuable and useful information. In an effort to assist transportation organizations, TSS partners have worked with members from DHS's Cybersecurity and Communications (CS&C) team to provide trend analysis. Categories for data collection were as follows:

- Tactics most commonly employed to gain illicit access to networks and systems.
- Vulnerabilities most frequently exploited in targeted systems and networks.
- Indicators of illicit cyber activities most often noted in post-incident analyses that were missed or disregarded.
- Protective measures most often found lacking or absent that could have made a difference – aligned with the tactics these measures either defeat or mitigate.

Recognizing that threats are dynamic and risk mitigation efforts need to be proactive and sustained, this Implementation Guidance calls for two recurring priorities: (1) annual joint requests by the TSS government and industry partners for updates on the cyber threat trend analyses as outlined above; and (2) application of the results, as appropriate, by transportation entities through periodic review of their assessed risk profile against the threat trends.

Applying Threat Information to Maturity Model

Organizations can amend their maturity levels to accurately depict their risk profile utilizing the information gathered through the completion of the internal context and the threat intelligence provided. The adjusted maturity levels are established based on the potential impact particular events have on the organization and how they affect the organization's mission, protection of assets, fulfillment of legal responsibilities, maintenance of day-to-day functions, protection of individuals, and the company's aversion to risk.

This TSS Implementation Guidance defines three levels of potential impact within a maturity model to organizations or domain areas should a security breach occur. The levels of impact are as follows:

- ***LOW*** – The organization or domain area would experience **limited** adverse effects based on the threat intelligence provided.
- ***MODERATE*** – The organization or domain area would experience **serious** adverse effects based on the threat intelligence provided.
- ***HIGH*** – The organization or domain area would experience **severe or catastrophic** adverse effects based on the threat intelligence provided.

Some items to take into consideration when performing self-adjustments to the indicator levels are as follows:

- A single, HIGH watermark in any of the four intelligence areas should be considered for auto adjustment of one color.
- A value of **Not Applicable** can be assigned per the organization's discretion.

Table 1 demonstrates how an organization can adjust established maturity indicator levels based on threat intelligence.

Table 1: Sample Maturity Adjustment Based on Threat Intelligence

Maturity Domain	MIL Result	Tactics	Vulnerabilities	Missed Activities	Protective Measures Missing	Maturity Level Recommended
Asset Management	MIL 1	Low	Low	Low	Low	MIL 1
Controls Management	MIL 3	Low	Moderate	Low	Low	MIL 2
Configuration and Change	MIL 3	Moderate	Low	Low	Moderate	MIL 1
Management	MIL 4	Low	Low	High	Low	MIL 2
Vulnerability Management	MIL 3	Low	Low	Moderate	High	MIL 1
Incident Management	MIL 3	High	Moderate	Moderate	Low	MIL 1
Service Continuity Management	MIL 5	Low	Low	Low	Moderate	MIL 4
Risk Management	MIL 2	Low	Low	Low	Low	MIL 2
External Dependencies Management	MIL 1	Moderate	High	Low	Low	MIL 1
Training and Awareness	MIL 5	Low	Moderate	Low	Low	MIL 4
Situational Awareness	MIL 2	Low	Low	Low	Low	MIL 2

Maturity Domain	MIL Result	Tactics	Vulnerabilities	Missed Activities	Protective Measures Missing	Maturity Level Recommened
Risk Management	MIL 3	Low	Moderate	Low	Low	MIL 2
Asset, Change, and Configuration Management	MIL 2	Moderate	Low	Moderate	Low	MIL 1
Identity and Access Management	MIL 4	Low	Low	Low	Low	MIL 4
Threat and Vulnerability Management	MIL 1	Low	Low	w	High	MIL 1
Situational Awareness	MIL 5	Low	Moderate	Low	Low	MIL 4
Information Sharing and Communications	MIL 3	Moderate	Moderate	Moderate	Moderate	MIL 1
Event and Incident Response, Continuity of Operations	MIL 3	Low	Low	Low	Low	MIL 3
Supply Chain and External Dependencies Management	MIL 2	Low	Low	Moderate	Low	MIL 1
Workforce Management	MIL 4	High	Low	Moderate	Low	MIL 2
Cybersecurity Program Management	MIL 1	Moderate	Low	Low	Low	MIL 1
Situational Awareness	MIL 2	Low	Moderate	Low	High	MIL 1

Phase 1 Outcome: Overall Conceptual Environment

Once the internal and external context has been established, an organization will have a much clearer picture of its risk profile, and where opportunities for improvement reside. Data generated from the current processes should be populated into the XXX spreadsheet attached in Appendix 2.

Phase 2: Establishing Priorities

Upon completion of Phase 1, the organization will be ready to pinpoint where opportunities reside and how to prioritize solutions to reduce its overall risk profile. When developing a strategy to implement solutions, the organization should take resource allocation (both personnel and financial) into account. Below are a few options to consider.

1. **Highest Risk First:** Items with the highest probability of affecting the organization are targeted first. These would be the items labeled in RED that were identified in Phase 1.
2. **Disruption to Business Operations:** Issues with a higher probability of affecting critical business functions are given more emphasis.
3. **Lowest Risk/Quickest Win:** In some cases, low risk issues requiring lighter resource allocation are given priority to obtain quick solutions.

Phase 3: Implementing Solutions

Appendix 1 contains current standards that can be used to assist organizations with implementing solutions to issues prioritized for remediation. All of these standards have slight differences and should be reviewed to ensure the guidance most suitable to reducing the organization's specific risk profile is selected.

Appendix 1: Resource Guide

The following list provides resources available to assist with the Implementation Guidance process.

Internal Context Assessment

Department of Homeland Security Cyber Resilience Review
https://www.us-cert.gov/ccubedvp/self-service-crr

Department of Energy C2M2 (many variations)
http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity

Priority-Based Assessment Tools

Department of Homeland Security Cyber Security Evaluation Tool
https://ics-cert.us-cert.gov/Assessments

NIST Publications

NIST 800-53
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST 800-82
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

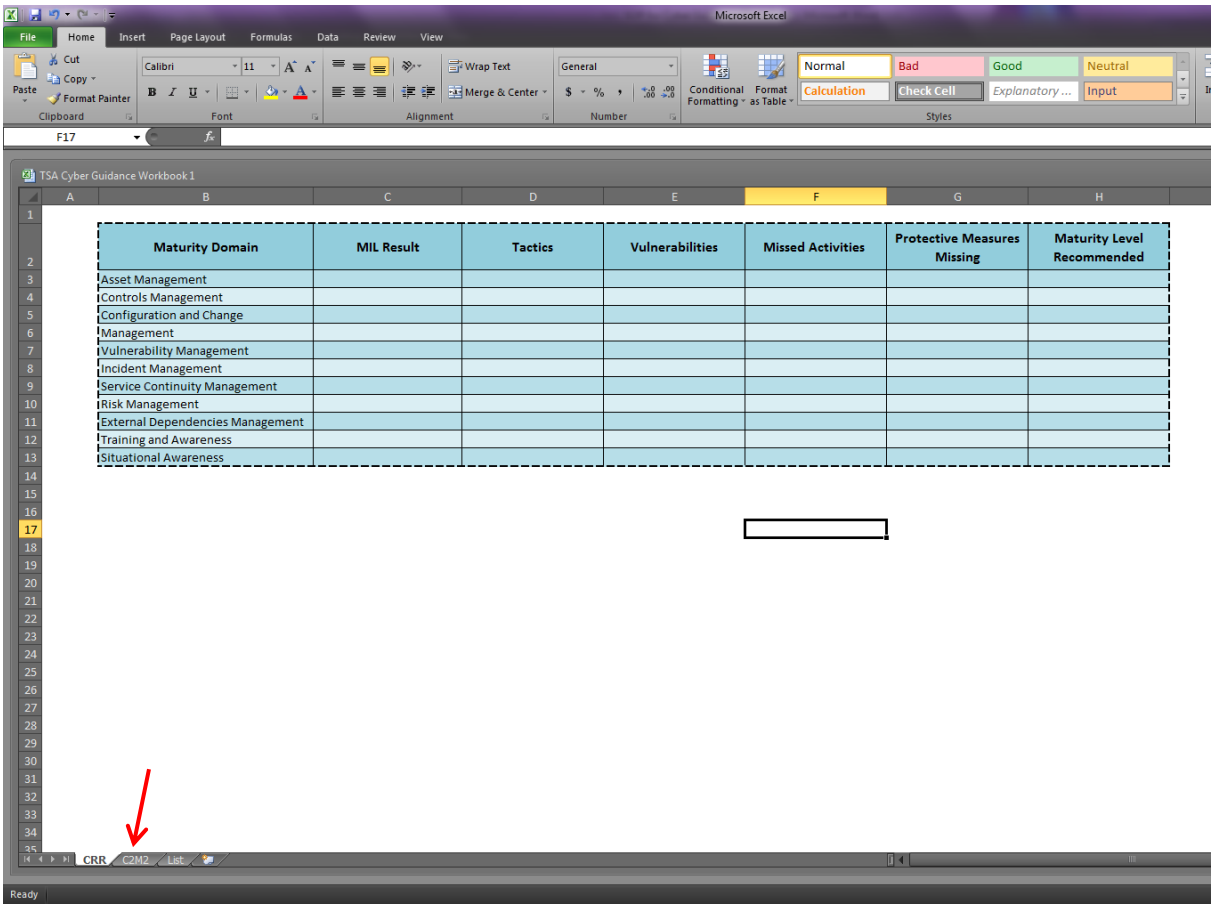
ISO/IEC 27001:2013

http://www.iso.org/iso/catalogue_detail?csnumber=54534

Appendix 2: Using the Risk Profile Adjustment Tool

Step 1:

Identify which assessment tool was used, either the Cyber Resilience Review (CRR) or the Cybersecurity Capability Maturity Model (C2M2). Open the workbook and select the correct sheet.



Maturity Domain	MIL Result	Tactics	Vulnerabilities	Missed Activities	Protective Measures Missing	Maturity Level Recommended
Asset Management						
Controls Management						
Configuration and Change Management						
Vulnerability Management						
Incident Management						
Service Continuity Management						
Risk Management						
External Dependencies Management						
Training and Awareness						
Situational Awareness						

To make the selection of the correct sheet they will be listed at the bottom of the worksheet.

Step 2:

Once the selection is made (CRR is going to be used for the example) the spreadsheet with options is available.

Maturity Domain	MIL Result	Tactics	Vulnerabilities	Missed Activities	Protective Measures Missing	Maturity Level Recommended
Asset Management						
Controls Management						
Configuration and Change Management						
Vulnerability Management						
Incident Management						
Service Continuity Management						
Risk Management						
External Dependencies Management						
Training and Awareness						
Situational Awareness						

Once you have done the assessment, it will give a MIL result. That is inputted in this column:

Maturity Domain	MIL Result	Tactics	Vulnerabilities	Missed Activities	Protective Measures Missing	Maturity Level Recommended
Asset Management						
Controls Management						
Configuration and Change Management						
Vulnerability Management						
Incident Management						
Service Continuity Management						
Risk Management						
External Dependencies Management						
Training and Awareness						
Situational Awareness						

MIL 1
MIL 2
MIL 3
MIL 4
MIL 5

MIL 1-5 is the options available through the drop down list.

Step 3:

Utilizing the information gathered through the completion of the CRR or C2M2 input the information to see where the highest threat is.

Maturity Domain	MIL Result	Tactics	Vulnerabilities	Missed Activities	Protective Measures Missing	Maturity Level Recommended
Asset Management	MIL 1	Low	Low	Low	Low	MIL 1
Controls Management	MIL 2	Low	Moderate	Low	Low	MIL 1
Configuration and Change Management	MIL 3	Moderate	Low	Low	Moderate	MIL 1
Management	MIL 4	Low	Low	High	Low	MIL 2
Vulnerability Management						
Incident Management						
Service Continuity Management						
Risk Management						
External Dependencies Management						
Training and Awareness						
Situational Awareness						

Low
Moderate
High

The recommended maturity level is auto populated depending on the choices that are picked (low, moderate, high).

******NOTE: Once completed with all risks work on bringing up maturity levels. Just because a low MIL level is green does not mean it is mature. ******

Example:

CRR

Maturity Domain	MIL Result	Tactics	Vulnerabilities	Missed Activities	Protective Measures Missing	Maturity Level Recommended
Asset Management	MIL 1	Low	Low	Low	Low	MIL 1
Controls Management	MIL 3	Low	Moderate	Low	Low	MIL 2
Configuration and Change	MIL 3	Moderate	Low	Low	Moderate	MIL 1
Management	MIL 4	Low	Low	High	Low	MIL 2
Vulnerability Management	MIL 3	Low	Low	Moderate	High	MIL 1
Incident Management	MIL 3	High	Moderate	Moderate	Low	MIL 1
Service Continuity Management	MIL 5	Low	Low	Low	Moderate	MIL 4
Risk Management	MIL 2	Low	Low	Low	Low	MIL 2
External Dependencies Management	MIL 1	Moderate	High	Low	Low	MIL 1
Training and Awareness	MIL 5	Low	Moderate	Low	Low	MIL 4
Situational Awareness	MIL 2	Low	Low	Low	Low	MIL 2

C2M2

Maturity Domain	MIL Result	Tactics	Vulnerabilities	Missed Activities	Protective Measures Missing	Maturity Level Recommened
Risk Management	MIL 3	Low	Moderate	Low	Low	MIL 2
Asset, Change, and Configuration Management	MIL 2	Moderate	Low	Moderate	Low	MIL 1
Identity and Access Management	MIL 4	Low	Low	Low	Low	MIL 4
Threat and Vulnerability Management	MIL 1	Low	Low	w	High	MIL 1
Situational Awareness	MIL 5	Low	Moderate	Low	Low	MIL 4
Information Sharing and Communications	MIL 3	Moderate	Moderate	Moderate	Moderate	MIL 1
Event and Incident Response, Continuity of Operations	MIL 3	Low	Low	Low	Low	MIL 3
Supply Chain and External Dependencies Management	MIL 2	Low	Low	Moderate	Low	MIL 1
Workforce Management	MIL 4	High	Low	Moderate	Low	MIL 2
Cybersecurity Program Management	MIL 1	Moderate	Low	Low	Low	MIL 1
Situational Awareness	MIL 2	Low	Moderate	Low	High	MIL 1