Cybersecurity: The NIST Framework Summarized

Mike Ockenga
Manager of IP Services

FINLEY ENGINEERING
INTEGRITY INTO EVERYTHING

The NIST Cybersecurity Framework

Big Goals

- Define Cybersecurity standards and practices
- Protect personal privacy and liberty
- Manage risk cost-effectively

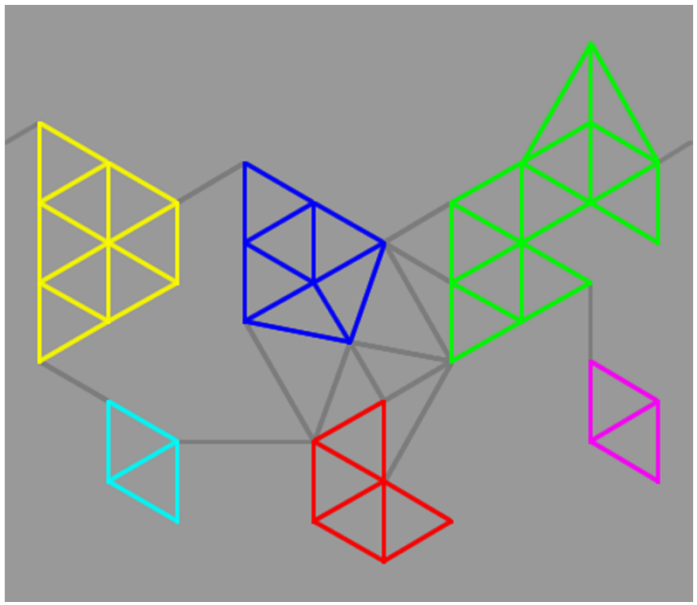
The NIST Cybersecurity Framework is the implementation of President Obama's Executive Order 13636 from 2013.

Mike Ockenga
m.ockenga@fecinc.om

The NIST Cybersecurity Framework

Important Points

- Voluntary not Regulatory
- Risk-focused
- Government-Private Collaboration
- Useful for all sized organizations
- Not a checklist



Mike Ockenga
m.ockenga@fecinc.om

The NIST Cybersecurity Framework

Three basic components

- Framework Core
- Framework Implementation Tiers
- Framework Profile

“The Framework provides a common language for understanding, managing and expressing cybyersecurity risk both internally and externally.” – Cybersecurity Framework Version 1.0

Mike Ockenga
m.ockenga@fecinc.om

The Four Elements of the Framework Core

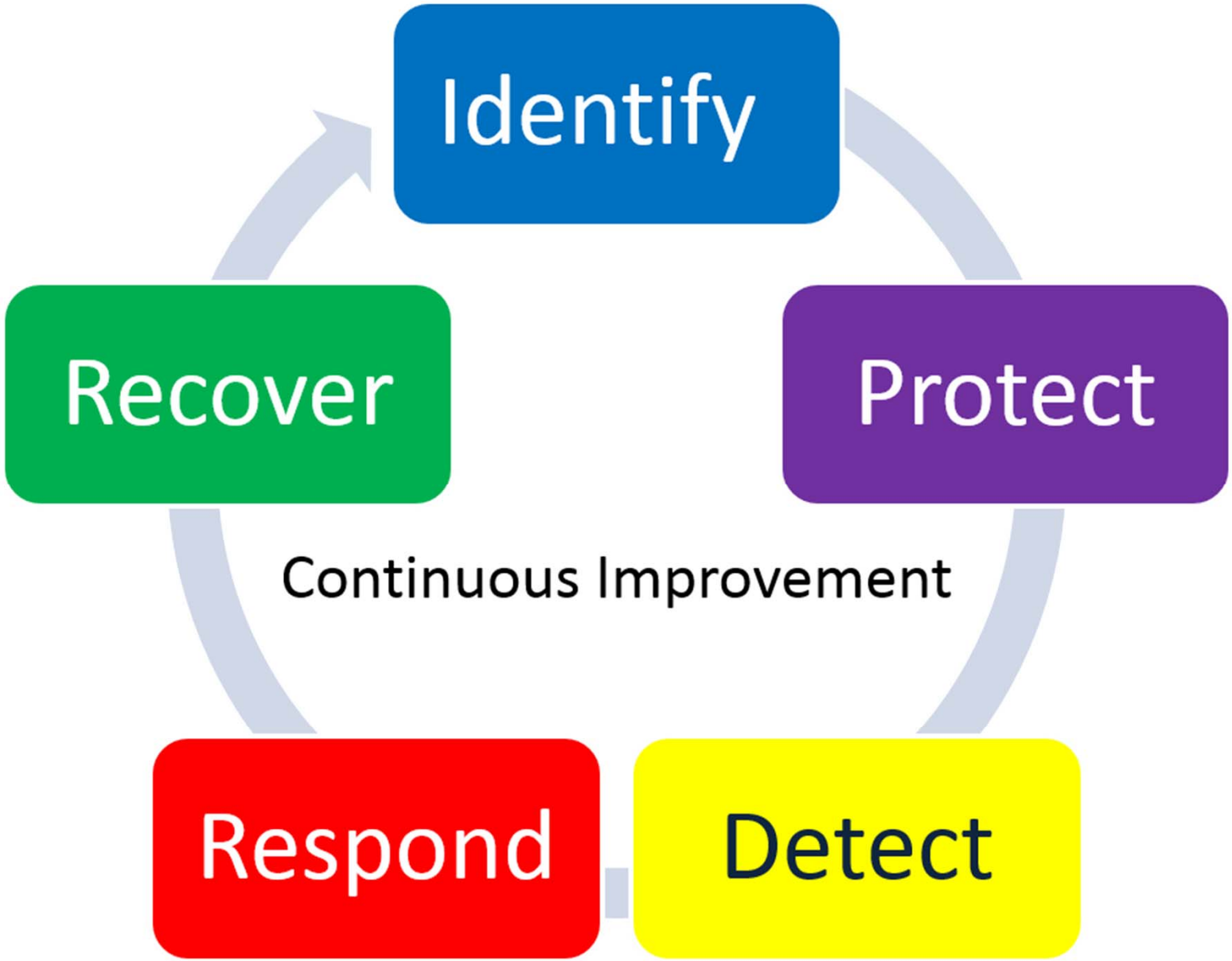
The Core Table

- Functions
- Categories
- Subcategories
- Informative References

Functions	Categories	Subcategories	Informative References
Identify			
Protect			
Detect			
Respond			
Recover			

These four elements are defined starting on page 7 of the Cybersecurity Framework Version 1.0.

Mike Ockenga
m.ockenga@fecinc.om


Identify
Protect
Detect
Respond
Recover
Continuous Improvement

Categories, Subcategories, and Informative References

Structuring your Activities

- Multiple Categories and Subcategories for each function
- Informative References are specific industry standards, best practices and guidelines applicable to each subcategorized function

“The Framework provides a common language for understanding, managing and expressing cybyersecurity risk both internally and externally.” – Cybersecurity Framework Version 1.0

Mike Ockenga
m.ockenga@fecinc.om

Building Context with Framework Implementation Tiers

Using four tiers to baseline your stance

- Tier 1: Partial
- Tier 2: Risk Informed
- Tier 3: Repeatable
- Tier 4: Adaptive

Mike Ockenga
m.ockenga@fecinc.om

What does “Tier 1: Partial” Mean?

There’s room for improvement

- Risk Management Process
  - Informal Practices
  - Ad hoc risk management
  - Activities not directly tied to business
- Integrated Risk Management Program
  - Limited cybersecurity awareness
  - Irregular or case-by-case handling
  - Likely little internal CS risk communication
- External Participation is limited

Mike Ockenga
m.ockenga@fecinc.om

What does “Tier 2: Risk Informed” Mean?

Headed the right way…

- Risk Management Process
  - Somewhat formalized practices
  - No organization-wide process yet
  - Priority activities are tied to business
- Integrated Risk Management Program
  - Awareness throughout organization, but no organization-wide program
  - Risk informed, management approved practices
  - Adequate resources and good communication
- External Participation
  - Organization understands its place the CS ecosystem
  - Formal external interactions are not established yet

Mike Ockenga
m.ockenga@fecinc.om

What does “Tier 3: Repeatable” Mean?

You’re doing well

- Risk Management Process
  - Organizational practices established as policy
  - Regularly updated based on risk management analysis of business changes
- Integrated Risk Management Program
  - Procedures, practices and policies established organization-wide
  - Methods are consistent and flexible
  - Staff capable and empowered
- External Participation
  - Organization understands partner dependencies
  - Exchanges information critical to risk analysis and mitigation activities

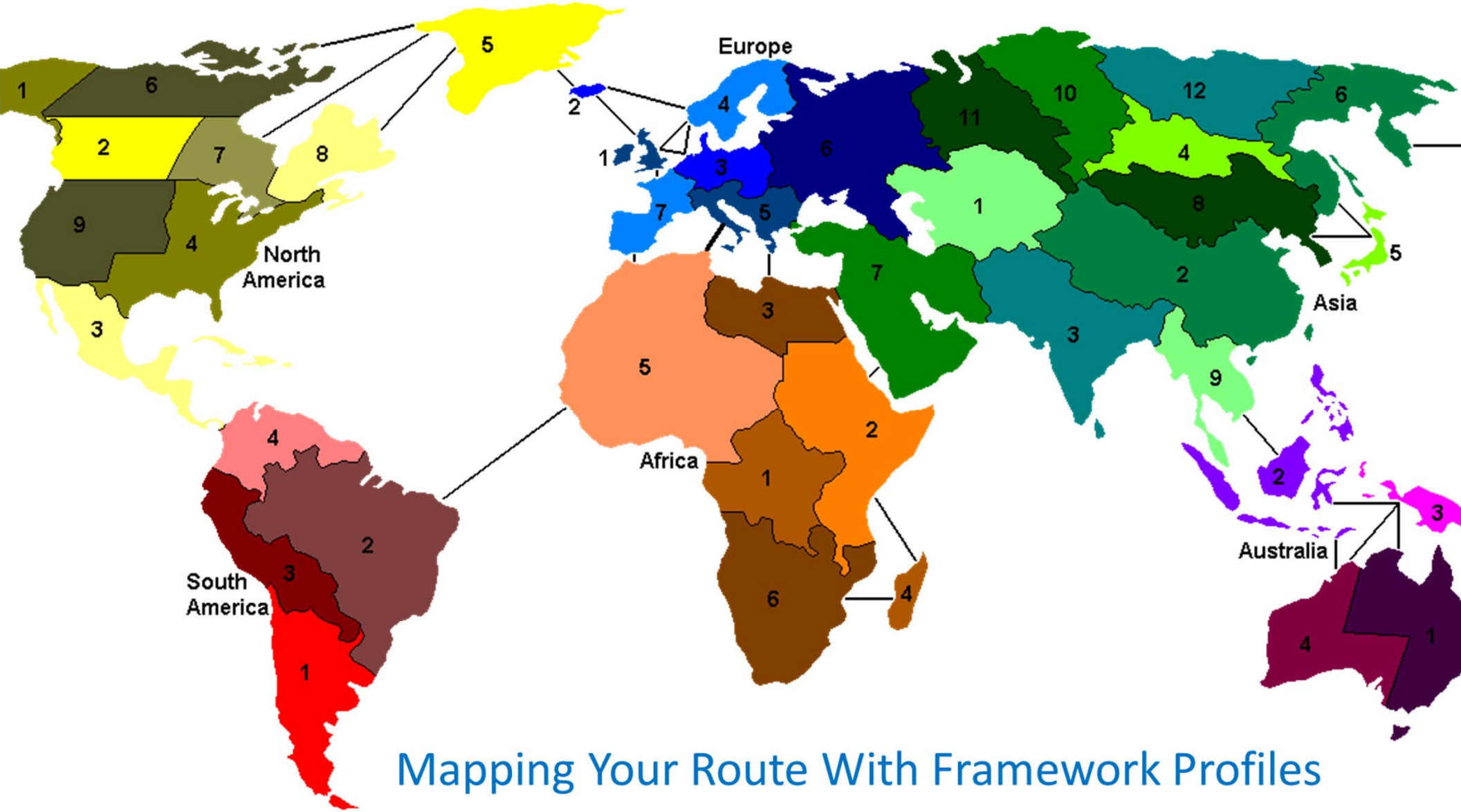
Mike Ockenga
m.ockenga@fecinc.om

What does “Tier 4: Adaptive” Mean?

You get the gold star

- Risk Management Process
  - Practices and policies continuously improve through lessons-learned and predictive analysis
  - Fluidly dapts to changing CS landscape
- Integrated Risk Management Program
  - CS practices and policies are cultural throughout organization
  - Programs evolve based on prior and current events, internal and external information, and constant awareness of CS state
- External Participation
  - Proactive information sharing
  - Fully integrated into policy and practices

Mike Ockenga
m.ockenga@fecinc.om



Mapping Your Route With Framework Profiles

Your Current and Target Profiles

Points on the map

- Profiles tie core elements to your specific business
- Your Current Profile is your start
- Your Target Profile is your goal given current conditions and business needs
- Continuous cyclical updates

Mike Ockenga
m.ockenga@fecinc.om

Links to visit for more information

- NIST Website
  - http://www.nist.gov/cyberframework/
  - Also has excel version of Core Element Table
- CForum (Blog) http://cyber.securityframework.org

Mike Ockenga
m.ockenga@fecinc.om

Thank you!

Mike Ockenga

Manager of IP Services
Finley Engineering Company, Inc.
m.ockenga@fecinc.com
952-223-8075