National Cyber Strategy Development & Implementation Framework – Assessment Phase

MITRE

Cyber Strategy Challenges

- Cyber strategy development is usually focused at the technical level.
- A cyber strategy should be integrated with national or organizational missions.

MITRE

MITRE's Cyber Strategy Capability

Provides strategic approaches to leverage the transformative characteristics of cyberspace and can be applied to diverse organizations and missions.

MITRE

Our Methodology - The NCSDI Framework

We examine 8 strategic areas across 2 levels of analysis to identify existing capacity and future aspirations, and to help develop approaches for closing prioritized gaps.

MITRE

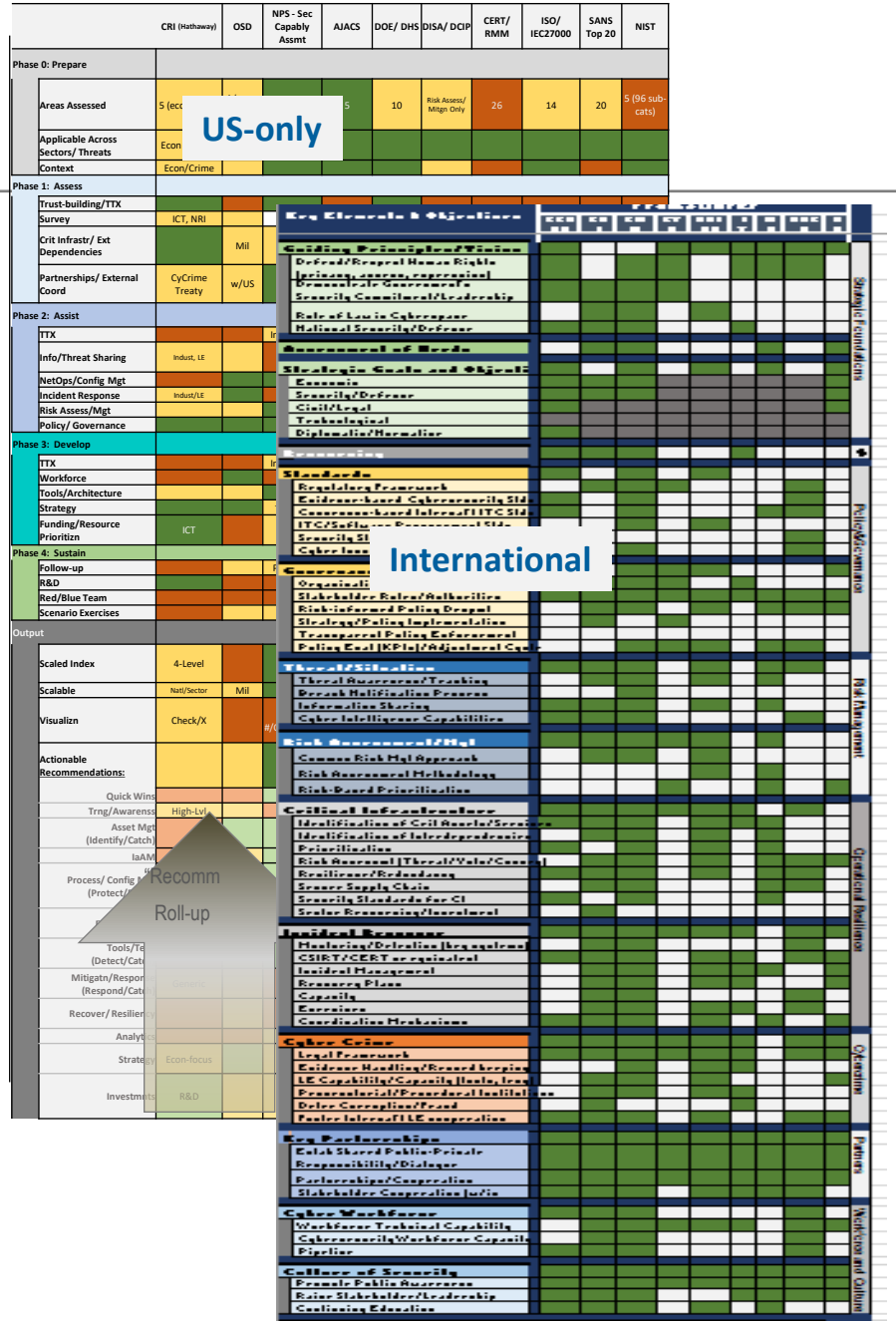
NCSDI Model Evolution

Compared 18 US and international cyber assessment methodologies

Identified key commonalities and best of breed attributes

Applied real-world lessons learned from previous international strategy work

Developed NCS Framework based on the 8 key capability areas that emerged



MITRE

Overview of the NCSDI Framework: Eight Key Elements

- **The Framework examines Cyber Strategies against eight key elements**

- **Executing the Framework through its Phases and Activities helps to determine a nation's, organization's or region's…**
  - Current capacity
  - Future goals and aspirations
  - Specific actions to help close gaps
  - Organizational psychology that affects sustained change

MITRE

Cyber Strategy is Implemented From the Ground Up

Key Partnerships
Public Awareness & Culture of Security
Cybersecurity Workforce Development

Enabling

Operational Resilience & Incident Response
Cybercrime Prevention & Response

Operational

Risk Management
Policy, Governance, & Resourcing

Governance

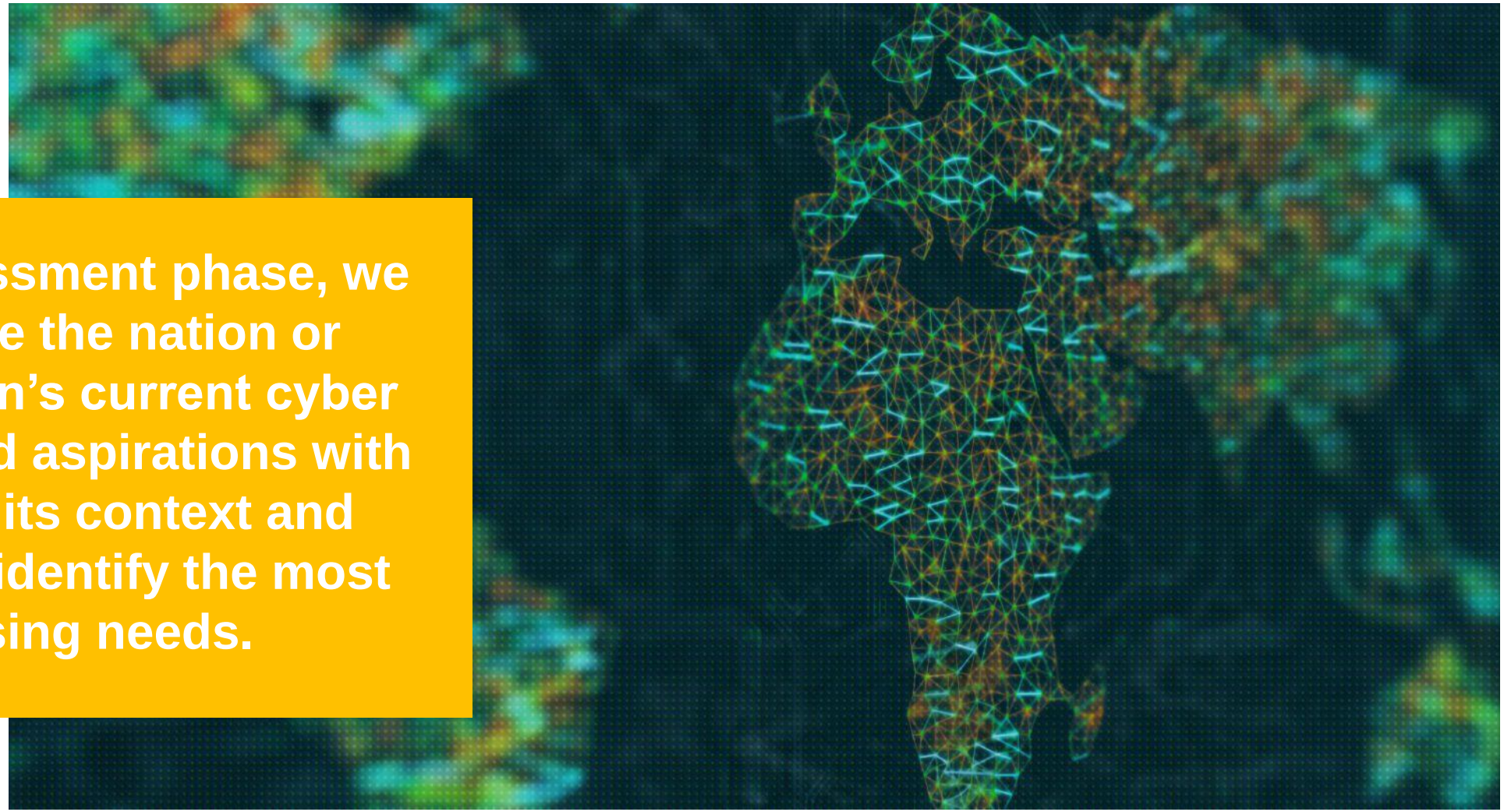
Strategic Foundations

Foundational

NCSDI Framework

MITRE

NCSDI Framework Phase 2: Assess



In the Assessment phase, we determine the nation or organization's current cyber capacity and aspirations with regard to its context and threats, to identify the most pressing needs.

MITRE

NCS Framework Phase 2: Assess

Determine the country's current capacity across the 8 Essential Elements…

… in the context of national cyber-related opportunities and risks/threats.

No pre-defined objectives—not a Maturity Model!

Results inform development of national Goals and Priorities

Preparatory Questions

8 Preparatory Questions on National Cyber Strategy Readiness

It is not uncommon for nations to have questions on where to start when beginning national-level strategic cyber planning. These Preparatory Questions are the place to begin and will help determine readiness for that planning, as well as draw out areas that may need some attention first, before planning can begin.

1. Is internet connectivity a significant part of the country's national development plan? That is, is internet infrastructure considered on a par with electricity, roads, water, etc.?

Why is this important? The lack of internet connectivity excludes billions of people from economic and knowledge benefits. Moreover, internet access is an essential pre-requisite for participation in the modern global economy, and in extending knowledge, services and access to expertise to underdeveloped areas.

2. Does a broad segment of the government (and all key decision makers) agree that cyber capacity building is a national priority?

Why is this important? Building and implementing an effective cyber strategy will require broad cross-government agreement about its importance. One reason for this is the interconnected nature of cyber capabilities and processes—it is difficult to implement new cyber capabilities in only part of the government or key industries, if those rely on the exchange of information with others. In addition, broad commitment is usually necessary in order to provide resources, coordinate implementation, and convincingly communicate cyber as a priority to the larger society.

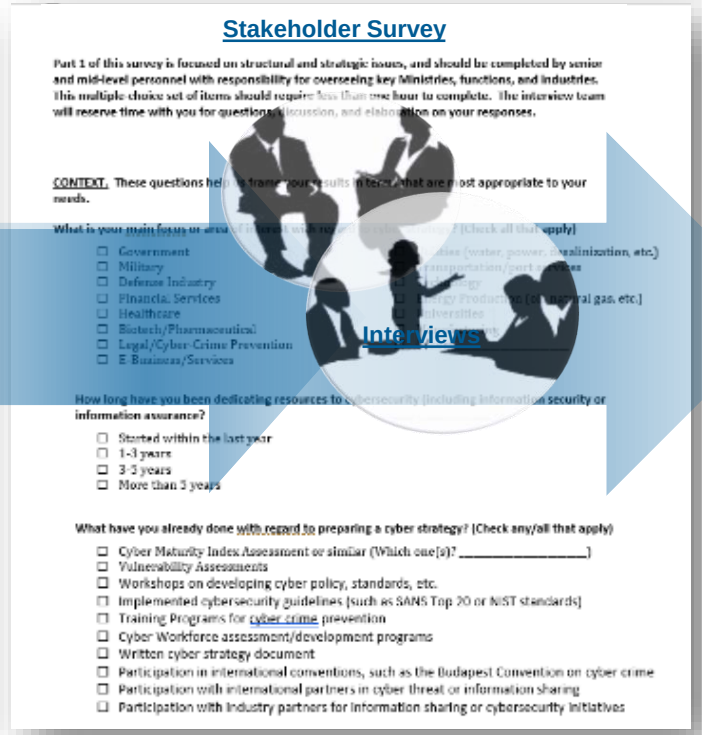
3. Does your country have a defined set of cybersecurity stakeholders?

Why is this important? Cyberspace cuts across and connects government, industry, academia, businesses, and individuals, and involves infrastructure, regulatory, technical, legal, and ethical issues. Having stakeholders at the table that represent all major affected entities is important to developing a strategy that meets whole-of-nation needs.

4. Have roles and responsibilities been identified for cybersecurity stakeholders?

Why is this important? An effective cyber strategy development process will require the assignment of various responsibilities to different entities, such as leaders in internal affairs, education, industry oversight, commerce, defense, technology and police/judiciary.

Stakeholder Survey



Part 1 of this survey is focused on structural and strategic issues, and should be completed by senior and mid-level personnel with responsibility for overseeing key Ministries, functions, and industries. This multiple choice set of items should require less than one hour to complete. The interview team will reserve time with you for questions, discussion, and elaboration on your responses.

CONTEXT. These questions help us translate your results in terms that are most appropriate to your needs.

What is your main focus or area of work? (Check all that apply)

- ☐ Government
- ☐ Military
- ☐ Defense Industry
- ☐ Financial Services
- ☐ Healthcare
- ☐ Biotech/Pharmaceutical
- ☐ Legal/Cyber Crime Prevention
- ☐ E-Business/Services

How long have you been dedicating resources to cybersecurity (including information security or information assurance?

- ☐ Started within the last year
- ☐ 1-3 years
- ☐ 3-5 years
- ☐ More than 5 years

What have you already done with regard to preparing a cyber strategy? (Check any/all that apply)

- ☐ Cyber Maturity Index Assessment or similar (Which one[s]? _____)
- ☐ Vulnerability Assessments
- ☐ Workshops on developing cyber policy, standards, etc.
- ☐ Implemented cybersecurity guidelines (such as SANS Top 20 or NIST standards)
- ☐ Training Programs for cyber crime prevention
- ☐ Cyber Workforce assessment/development programs
- ☐ Written cyber strategy document
- ☐ Participation in international conventions, such as the Budapest Convention on cyber crime
- ☐ Participation with international partners in cyber threat or information sharing
- ☐ Participation with industry partners for information sharing or cybersecurity initiatives

Interviews

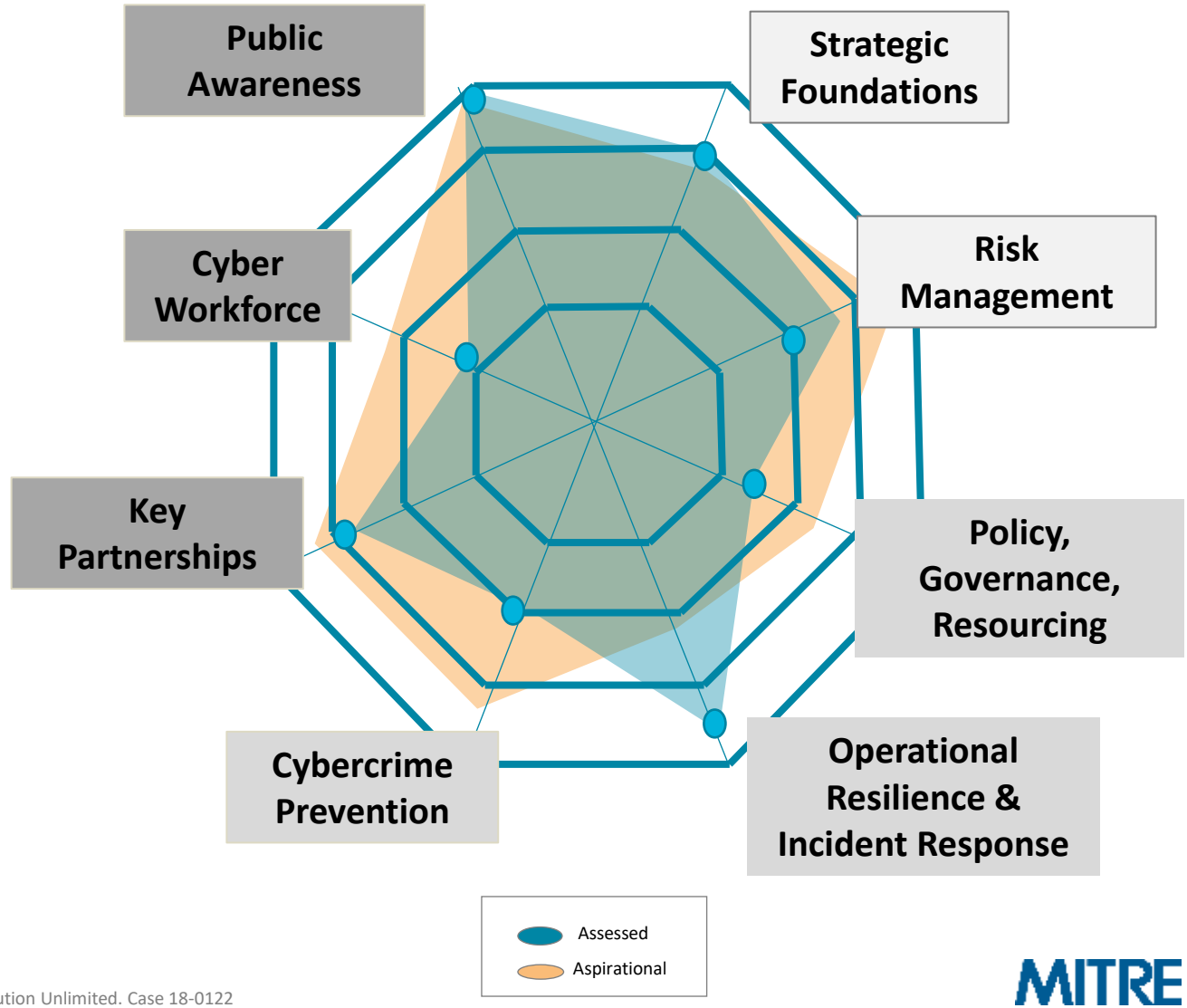
Tabletop Exercise

	X	1	2	3	4
STRATEGY FOUNDATIONSS	20	13	17	32	2
Documented Cyber Strategy	0	0	0	13	0
Scope of Strategy	2	0	10	1	0
Scope of CISO authority	1	5	0	10	0
CISO access to leadership?	5	5	5	0	0
Interdepartmental communication	9	3	1	1	
CYBER POLICY AND GOVERNANCE	23	10	12	22	4
Defined responsibility for national policy	5	3	7	0	1
Network security policy standardization	8	3	1	3	0
Standards for network usage	5	4	1	4	1
Defined responsibility for ITC	0	0	0	13	0
Asset tracking	5	0	3	2	2
RESOURCING	28	14	20	4	6
Ability to dedicate funds	5	3	2	0	3
Resource allocation schema	6	2	5	1	2
Alignment/integration of cyber funding	6	2	4	3	0
Scope of cyber funding (what's funded)	4	2	7	0	0
Budget projection timeframe	7	5	2	0	1
RISK MANAGEMENT	24	24	22	22	9
Critical dependency analysis	1	3	3	1	6
Controls for foreign cyber security risks	2	6	3	2	0
Threat/likelihood assessment	2	6	2	5	0
Threat awareness	0	2	5	7	2
Threat communication sources	5	3	6	1	0
Internal/External threat sharing practices	5	1	2	5	1
Self-assessment: nat'l threat sharing	9	3	1	1	0
OPERATIONAL RESILIENCY	41	23	11	7	4
Critical Infrastructure identification	2	1	1	10	4
Critical Infrastructure mapping	5	3	2	0	4
Confidence in secure crit infrastructure	5	2	3	5	0
Contingency planning	5	8	1	0	0
Escalation and response procedures	7	2	4	1	0
CSIRT capabilities	7	7	0	1	0
Cyber defense resources	12	1	1	0	0
KEY PARTNERSHIPS	22	1	6	8	18
Desire for Internal partnerships	7	0	2	1	2
Identification of internal partners	1	1	1	6	5
Desire for International partnerships	4	0	3	0	8
Identification of ext/internat'l partners	10	0	0	1	3
CYBERSECURITY CULTURE AND WORKFORCE	38	55	9	15	2
National leadership emphasis on cyber	4	3	0	6	2
Effectiveness of user awareness training	3	10	1	1	0
Metrics for effectiveness of user security	5	8	1	0	0
Gov's role in educating private citizens	8	5	1	1	0
Organic availability of cyber workforce	3	12	0	1	0
Workforce development plan	3	5	1	4	0

MITRE

Phase 2: Products

- A graphic representation of data displays **current capacity against goals and aspirations**
- No right or wrong answers in the Assessment Phase
- Scoring is done by a panel on a 0-4 scale - data in each category is rolled up to determine category "average"
- Survey data is validated by TTX and Preparatory Questions
- Assessment is captured in detailed report with **Recommendations**



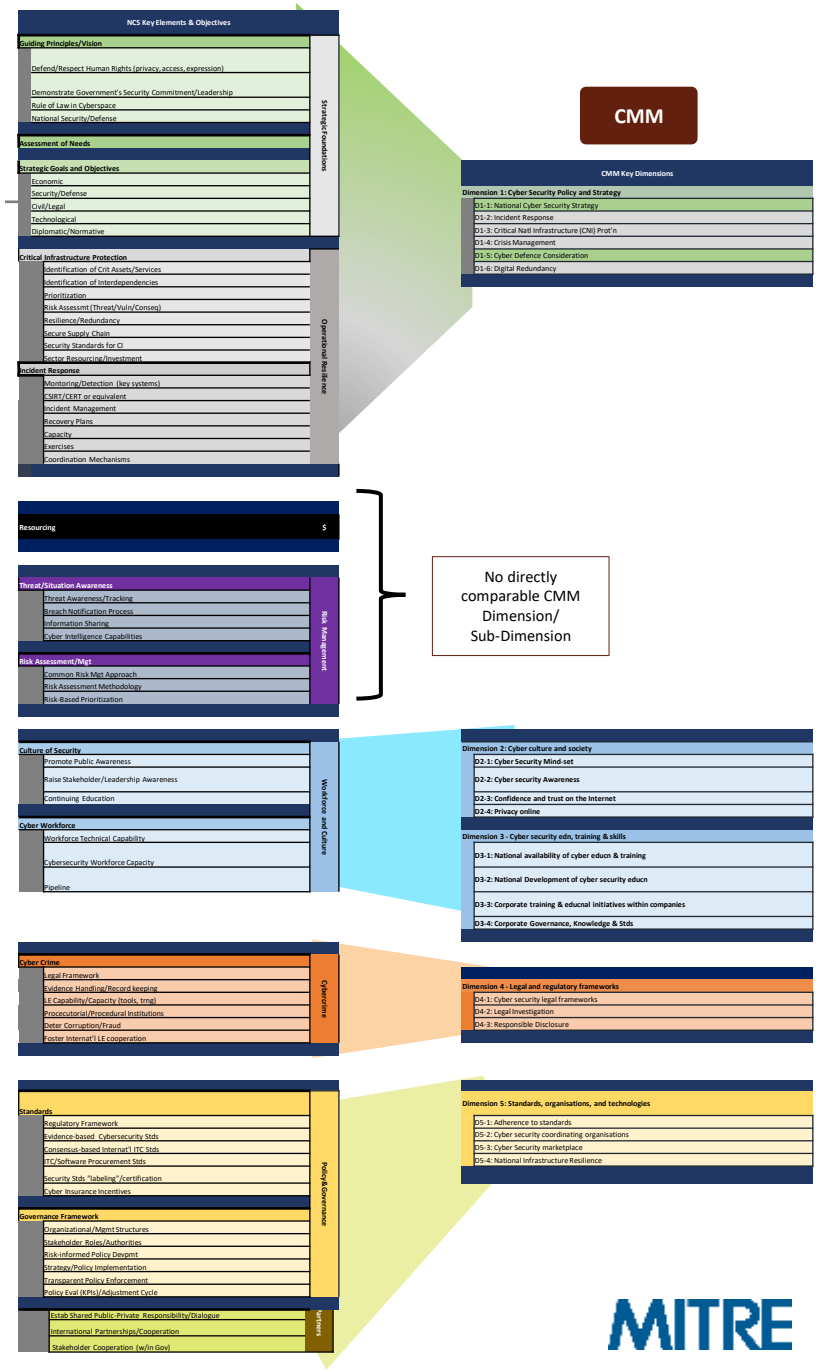
MITRE

High-Level NCS-CMM Comparison Conclusions (2016)

- **Both NCS and CMM were developed to include the best aspects of other leading strategy assessment/development models, so it is not surprising that there is a great deal of overlap**
- **In general, the CMM sets a more normative tone in that it uses a single Maturity Model for all contexts. The NCSDI is intended to reflect the unique needs and circumstances of a given country, without making comparisons to other countries or to a particular standard.**
- **CMM focuses more on national security elements of cyber-security, while the NCSDI model also looks at cyber-related economic opportunities and investments, including resourcing, in the context of other national needs/goals**
- **Accordingly, NCS uses indicators suggested by other models, such as CRI 2.0's economic context and focus on resourcing, Microsoft's emphasis on a national risk management approach, CCDOE's focus on strategic goal setting in several economic/security areas, etc.**

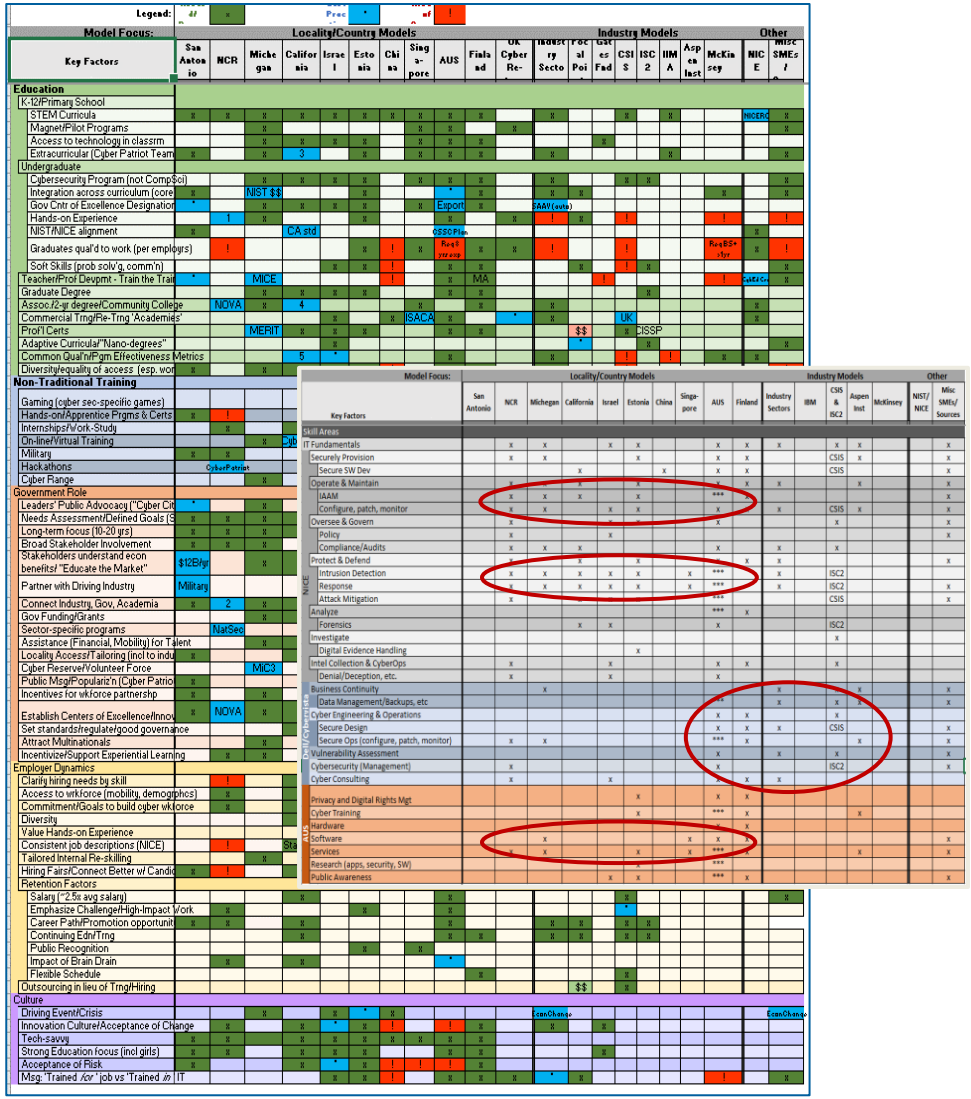
NCS-CMM Comparison Overview

- **The NCSDI model evaluates 8 areas:**
  - Strategy Foundations
  - Policy, Governance, Resourcing
  - Risk Management
  - Resiliency & Incident Response
  - Operational Resiliency
  - Cyber-Crime
  - Key Partnerships
  - Workforce Development
  - Cyber-security Culture/Awareness
- **Oxford's CMM evaluates 5 Key Dimensions:**
  1. Cyber-security Policy and Strategy
  2. Cyber-security Culture and Society
  3. Cyber-security Education, Training, and Skills
  4. Legal and Regulatory Frameworks
  5. Standards, Organizations, and Technologies
- **While specific sub-elements vary, there is significant overlap overall between CMM's elements and the NCSDI (some elements are grouped differently)**
- **In two areas (Culture, Education/Training/), the CMM looks at factors (privacy/ corporate standards) not directly addressed in the NCSDI, although Privacy Protections are addressed in NCSDI under Strategic Foundations (goals)**
- **NCSDI addresses 2 additional areas of focus as separate categories (Resourcing, Risk Management), though he CMM includes risk mgt as an element in protection of critical national infrastructure and standards**



MITRE

Coming Soon: Cyber Workforce Development Framework



- **Broad survey of tech workforce development approaches**
  - Nations of various size, economy
  - US States with different economic bases
  - Development NGOs (World Bank, Gates Foundn)
  - Economic Experts (McKinsey, Aspen Institute)
  - Cybersecurity SMEs (ISC2, CSIS, NICE)
- **Identified commonalities, needs, and best practices in 5 categories:**
  - Traditional Education (K-12 and college/university)
  - Other Training/Education approaches
  - Employer Inputs
  - Government Role
  - Cultural Factors
- **Synthesized into Framework focused on key areas and approaches for building cyber workforce capacity**

Approved for Public Release. Distribution Unlimited. Case 18-0122

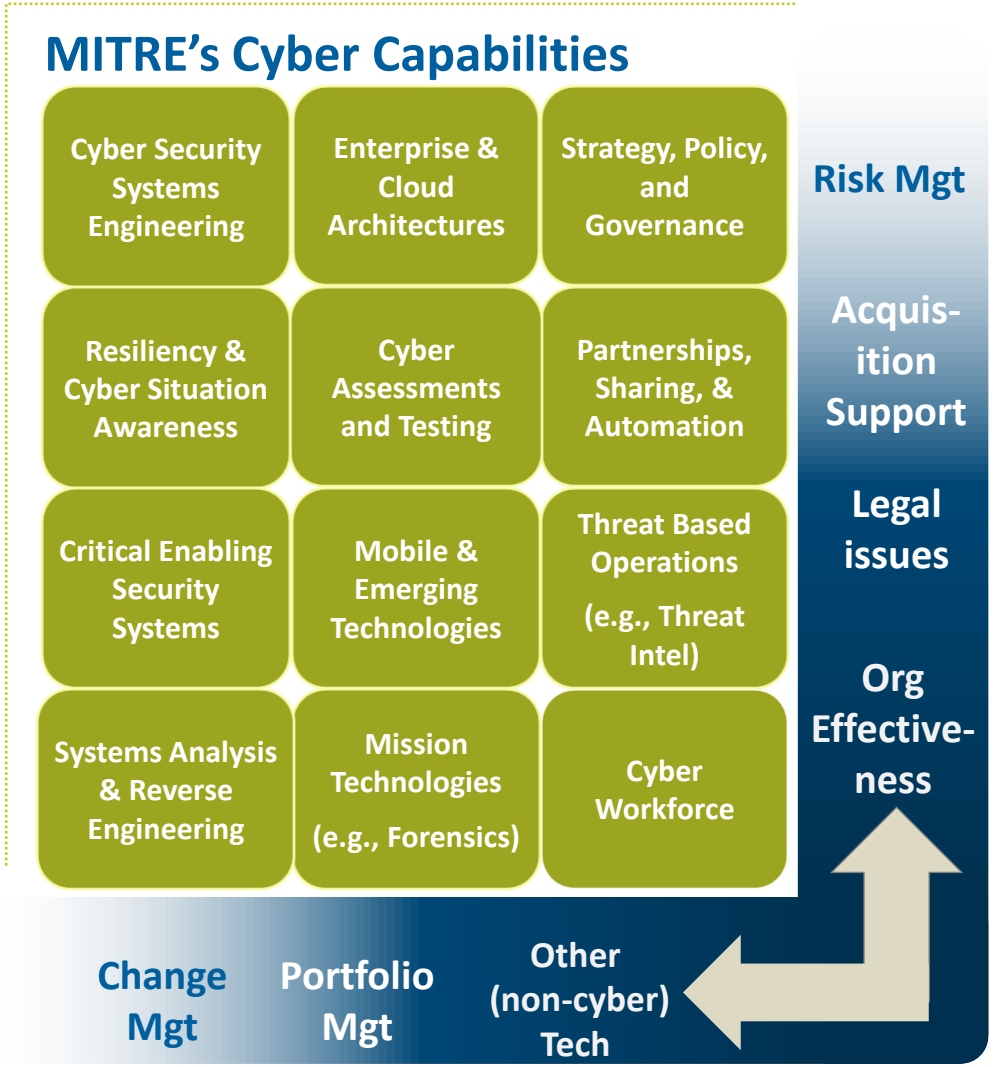
MITRE

Assessment is the Beginning…
(Assess, Assist, Develop, and Sustain)

MITRE provides a full range of capabilities necessary to support the complete CAAP framework

When needed, MITRE partners with other organizations or experts to augment our staff

Additional information available upon request



MITRE

QUESTIONS?