Cybersecurity Risk Management:

Building a Culture of Responsibility

G7 ICT and Industry Multistakeholder Conference

September 25 2017

Adam Sedgewick
asedgewick@doc.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Cybersecurity in the Department of Commerce

To create the conditions for economic growth and opportunity.

As part of the Administration's economic team, the Secretary of Commerce serves as the voice of U.S. business within the President's Cabinet.

- Trust can't be imposed on a marketplace.
- There is no single solution for addressing security concerns in cyberspace.
- Every Bureau Plays a Role

National Institute of Standards and Technology (NIST)

About NIST

- NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
  - 3,000 employees
  - 2,700 guest researchers
  - 1,300 field staff in partner organizations
  - Two main locations: Gaithersburg, MD and Boulder, CO

NIST Priority Research Areas


Advanced Manufacturing


IT and Cybersecurity


Healthcare


Forensic Science


Disaster Resilience


Cyber-physical Systems


Advanced Communications

Cybersecurity and the Digital Economy

"To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft."

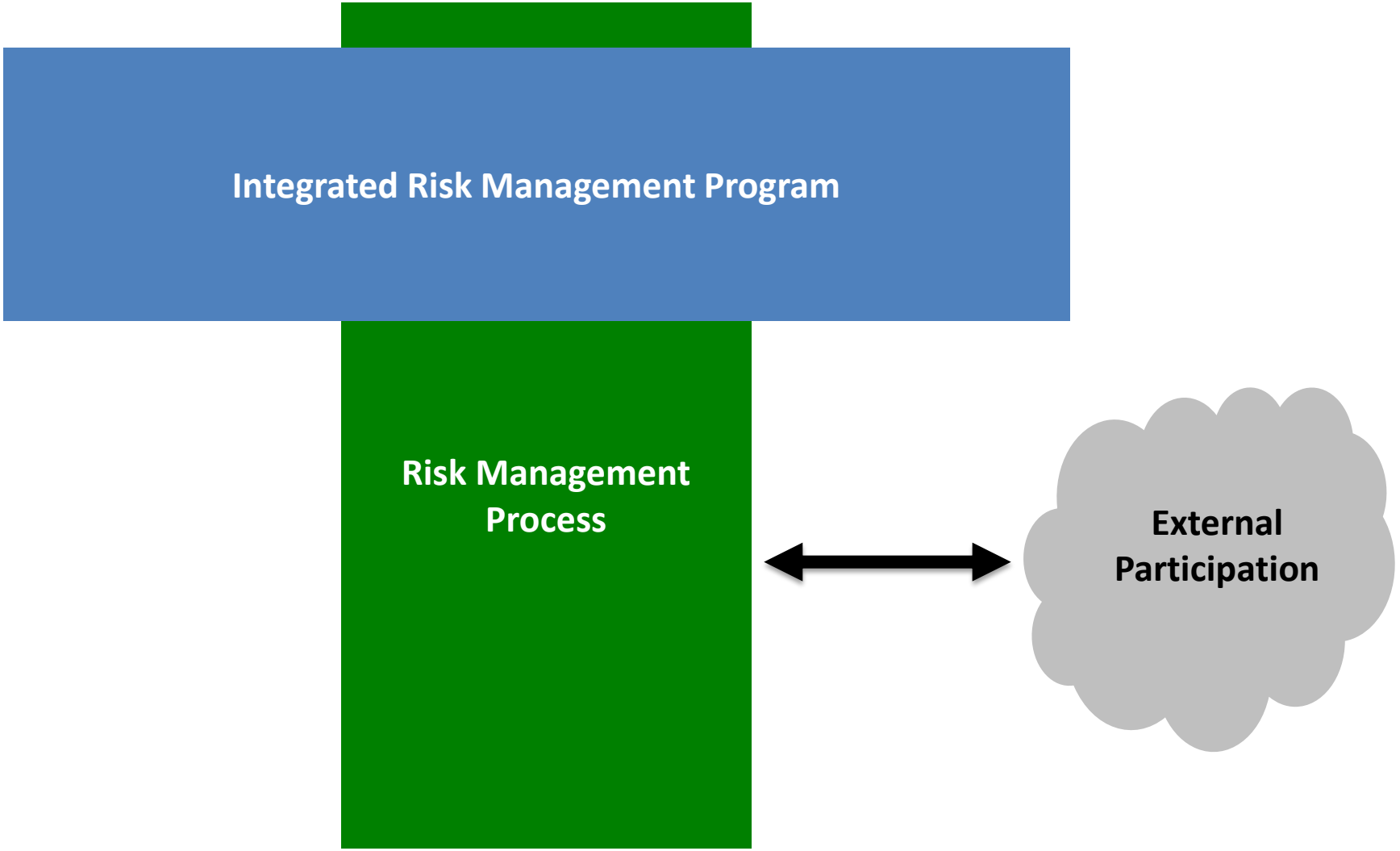
Executive Order 13800

11 May 2017

Approach to Organizational Risk Management: The Cybersecurity Framework

- Developed for CI, now used by organizations of any size, in any sector.
- That already or don't yet have a mature cyber risk management and cybersecurity program
- With a mission of helping keep up-to-date on managing risk and facing business threats

Key Properties of Cyber Risk Management



Example Approach in the CSF: Implementation Tiers

	1	2	3	4
	Partial	**Risk Informed**	**Repeatable**	**Adaptive**
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization benefits my sharing or receiving information from outside parties			

Key Attributes of the Approach

It's voluntary

- Is meant to be *customized*.

It's a framework, not a prescriptive standard

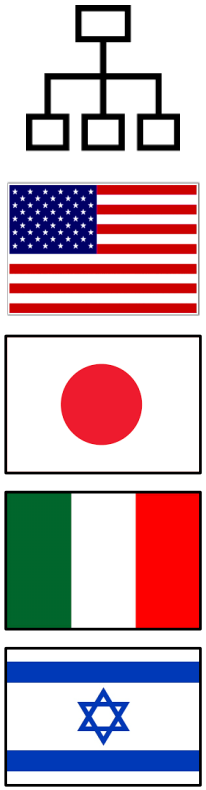
- Provides a *common language* and systematic methodology for managing cyber risk.
- Does not tell an organization *how* much cyber risk is tolerable, nor provide "the one and only" formula for cybersecurity.
- Enable best practices to become *standard practices* via common lexicon to enable action across diverse stakeholders.

It's a living document

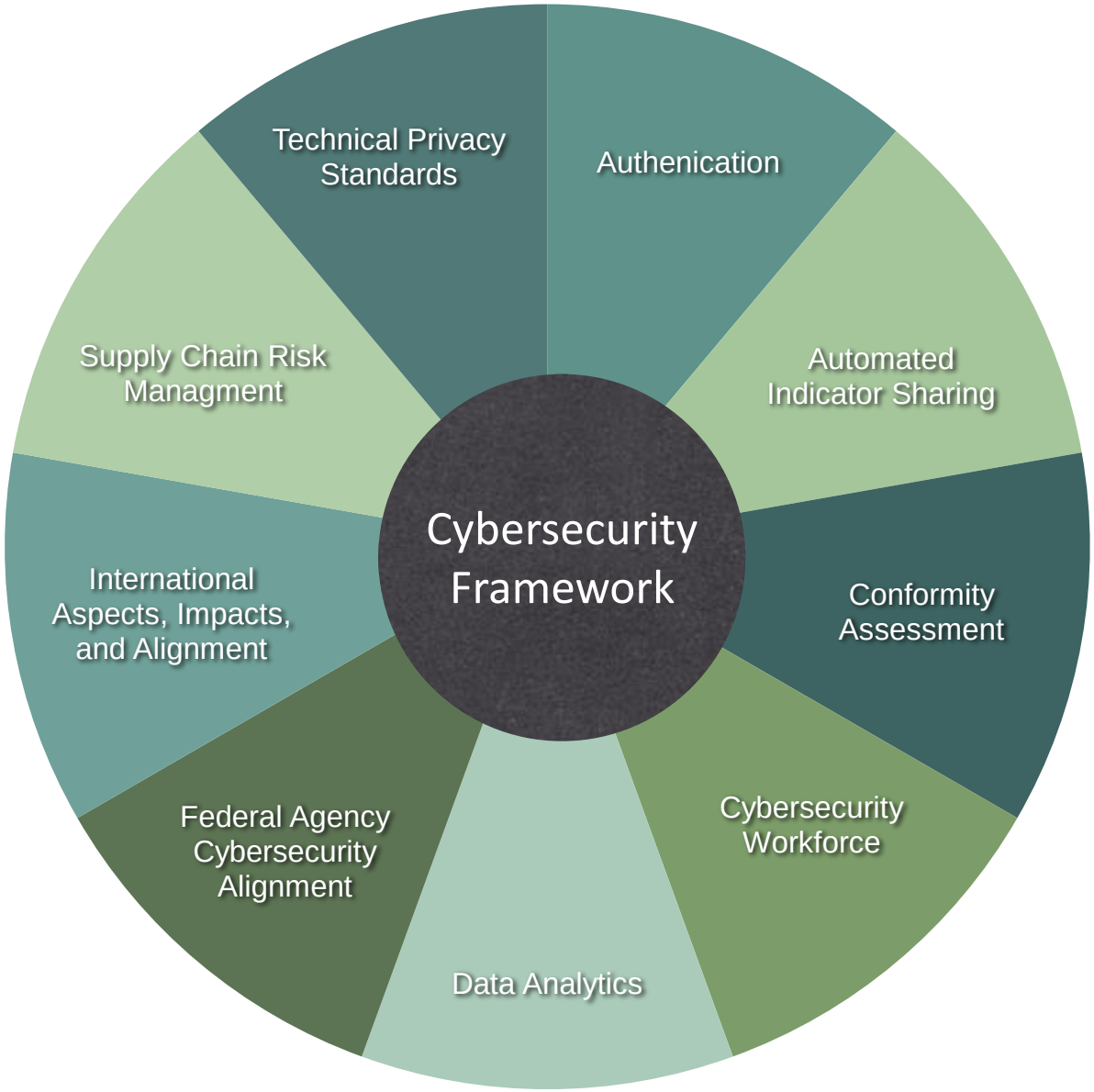
- Can be updated as stakeholders *learn from implementation*
- Can be updated as *technology and threats* changes.

International Uses of the CSF

- Used by over 30% of U.S. organizations, trending to 50% (per Gartner)
- Includes many Multinational Corporations
- Used by international governments and orgs:
  - Japanese translation by IPA
  - Italian adaptation within Italy's National Framework for Cybersecurity
  - Hebrew adaptation by Government of Israel
- ISO/IEC Study Periods and Technical Reports
  - Proposed Draft Technical Report ISO 27103



Continued Projects to Support CSF Use



Expanding Resources

www.nist.gov/cyberframework/industry-resources

Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Self-Assessment Criteria

Baldrige Cybersecurity Excellence Builder

Maritime Profile

U.S. Coast Guard Bulk Liquid Transport Profile

National Initiative for Cybersecurity Education

- EO 13800: “the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace”
- Strategic Goals:·
  - Accelerate Learning and Skills Development·
  - Nurture a Diverse Learning Community·
  - Guide Career Development and Workforce Planning

U.S. Strategic Engagement in International Cybersecurity Standards

- To ensure cybersecurity and resiliency of U.S. information and communications systems and supporting infrastructures, we must develop and use robust cybersecurity standards and assessment schemes.
- Four key (and interrelated) objectives for standards and assessment:
  - Enhancing national and economic security and public safety
  - Ensuring standards and assessment tools are technically sound
  - Facilitating international trade
  - Promoting innovation and competitiveness
- Standards developing bodies that develop standards through open, transparent, impartial, and consensus-based processes and are globally relevant are strongly preferred.

Resources

Where to Learn More and Stay Current

The National Institute of Standards and Technology Web site is available at http://www.nist.gov

NIST Computer Security Division Computer Security Resource Center is available at http://csrc.nist.gov/

The *Framework for Improving Critical Infrastructure Cybersecurity* and related news and information are available at www.nist.gov/cyberframework

For additional Framework info and help
cyberframework@nist.gov