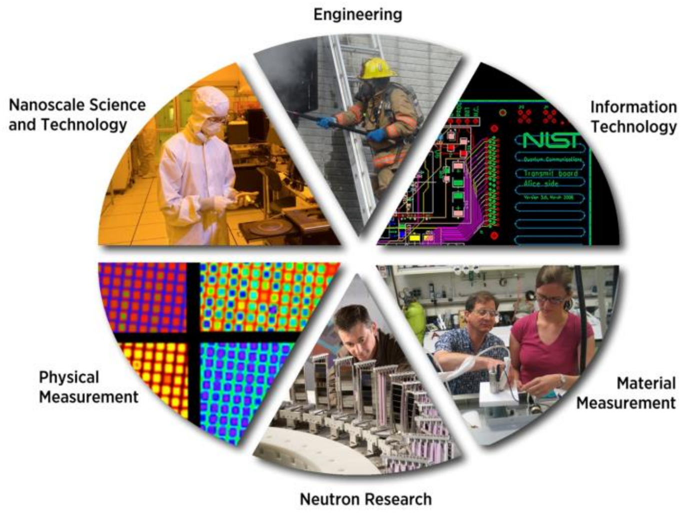
THE CONNECTED FUTURE: CHALLENGES AND OPPORTUNITIES

Cybersecurity Opportunities and Concerns in the New Interconnected Age

Kevin Stine, Chief, Applied Cybersecurity Division, NIST

National Institute of Standards and Technology



- 3,000 employees
- 2,700 guest researchers
- 1,300 field staff in partner organizations
- Two main locations: Gaithersburg, MD and Boulder, CO

Priority Research Areas

Advanced Manufacturing

IT and Cybersecurity

Healthcare

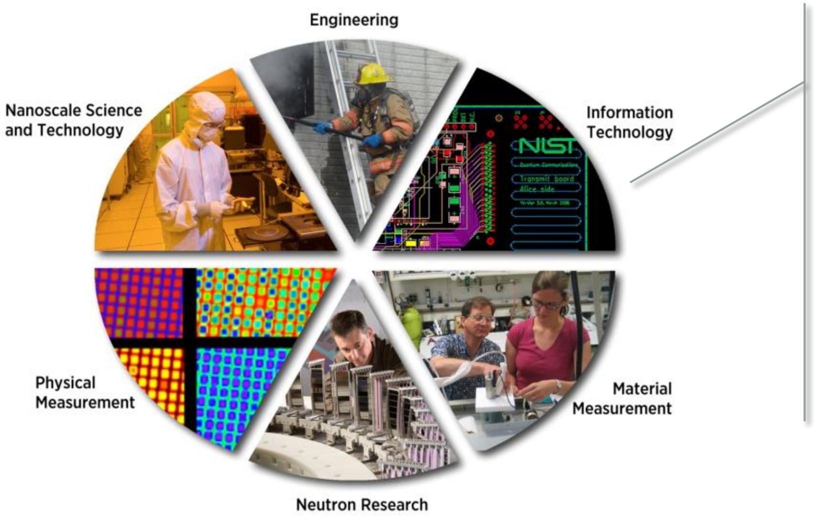
Forensic Science

Disaster Resilience

Cyber-physical Systems

Advanced Communications

NIST’s Cybersecurity Portfolio



Research, develop, and apply practical, innovative security technologies and methodologies that enhance our ability to address current and future computer and information security challenges.

Biometrics – Software Assurance – Domain Name Security – Identity Management – FISMA – Security Automation – National Vulnerability Database – Configuration Checklists – Digital Signatures – Risk Management – Authentication – IPv6 Security Profile – Supply Chain – NICE – Health IT Security – Key Management – Secure Hash – PKI – Privacy Engineering– Smart Grid – Continuous Monitoring – Small Business Outreach – Mobile Devices – Standards – Cloud Computing – Usability – NSTIC – Passwords – Hardware Security – Electronic Voting – Wireless – Security Awareness – Vulnerability Measurement – Security Metrics – Public Safety Communications – NCCoE

Cybersecurity requires a collaborative approach

- It is a cross-cutting problem, impacting Federal agencies, state and local governments, academia, all industries and market segments, consumers, and other countries.
- It is a national security, homeland security, economic security, law enforcement, technology, and people issue – *and innovation opportunity* - all at once.
- It requires a combination of technology, policy, people, and legal tools.

Challenges for Cities - Transportation

- Gridlock

- Limited room to build more roads

- Sprawl contributes to gridlock by increasing travel distance and time

- These vehicles have to be stored somewhere

Challenges for Cities - Energy

- Significant Energy Needs
  - Cities consume about 75% of all energy
  - Responsible for 40-60% of all greenhouse gases
- Aging Grids Supplying More People
- Need for More Sources of Power
  - Sustainable
  - Alternative to fossil fuel
  - Local

Challenges for Cities – Health and Mortality

- Air Quality
  - Researchers have defined “black rivers” of pollution in urban areas
    - Increase in incidence of respiratory disease
- Emergency Response
  - Delay caused by congestion
  - Lack of data in a timely manner can impede efficient response
- Water Management
  - Aging infrastructure that is not readily accessible
  - Essential to all life

The Smart Cities Initiative

Launched September 14th, 2015 and expanded in September 26th, 2016, to **target federal resources to meet local needs and support community-led solutions**

Goals

- Invest over **$160 million** in federal research in Sept 2015
- Additional **$80 million** announced Sept 2016
- Leverage dozens of new technology collaborations to help local communities tackle key challenges

Programs

- NIST (Global City Teams Challenge), NSF (Foundational Research)
- DHS, DOT, DOE, ITA, NTIA, EPA
- Formation of **Federal Smart Cities and Communities Task Force** for interagency cooperation

Global City Teams Challenge

NIST

GLOBAL CITY TEAMS CHALLENGE

usignite

- Establish and demonstrate replicable, scalable and sustainable models for collaborative incubation and deployment of interoperable, standard-based IoT solutions and demonstrate their *measurable* benefits in Smart Communities/Cities
- Enable the measurement science for real-world IoT deployments in scale

Advanced Technologies and Smart Cities

Technology convergence will revolutionize transportation, dramatically improving safety and mobility while reducing costs and environmental impacts

- Connected Vehicles
- Vehicle Automation

- Internet of Things
- Machine Learning
- Big Data
- Mobility on Demand

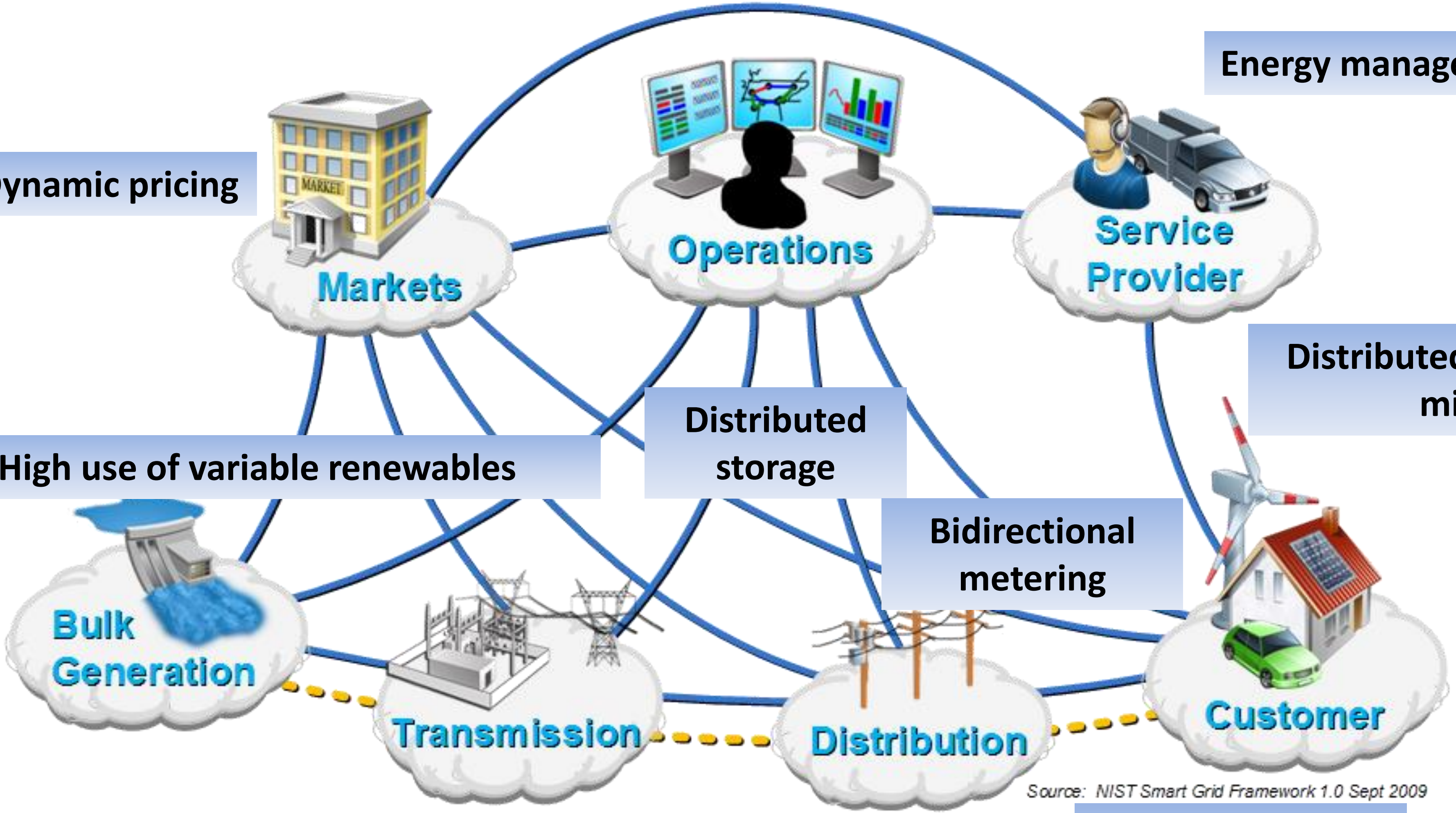
Connected-Automated Vehicles

Smart Cities

Benefits

- Order of magnitude safety improvements
- Reduced congestion
- Reduced emissions and use of fossil fuels
- Improved access to jobs and services
- Reduced transportation costs for gov't and users
- Improved accessibility and mobility

Smart Grid for Smart Cities



Source: NIST Smart Grid Framework 1.0 Sept 2009

Energy management systems

Dynamic pricing

Distributed generation and microgrids

High use of variable renewables

Distributed storage

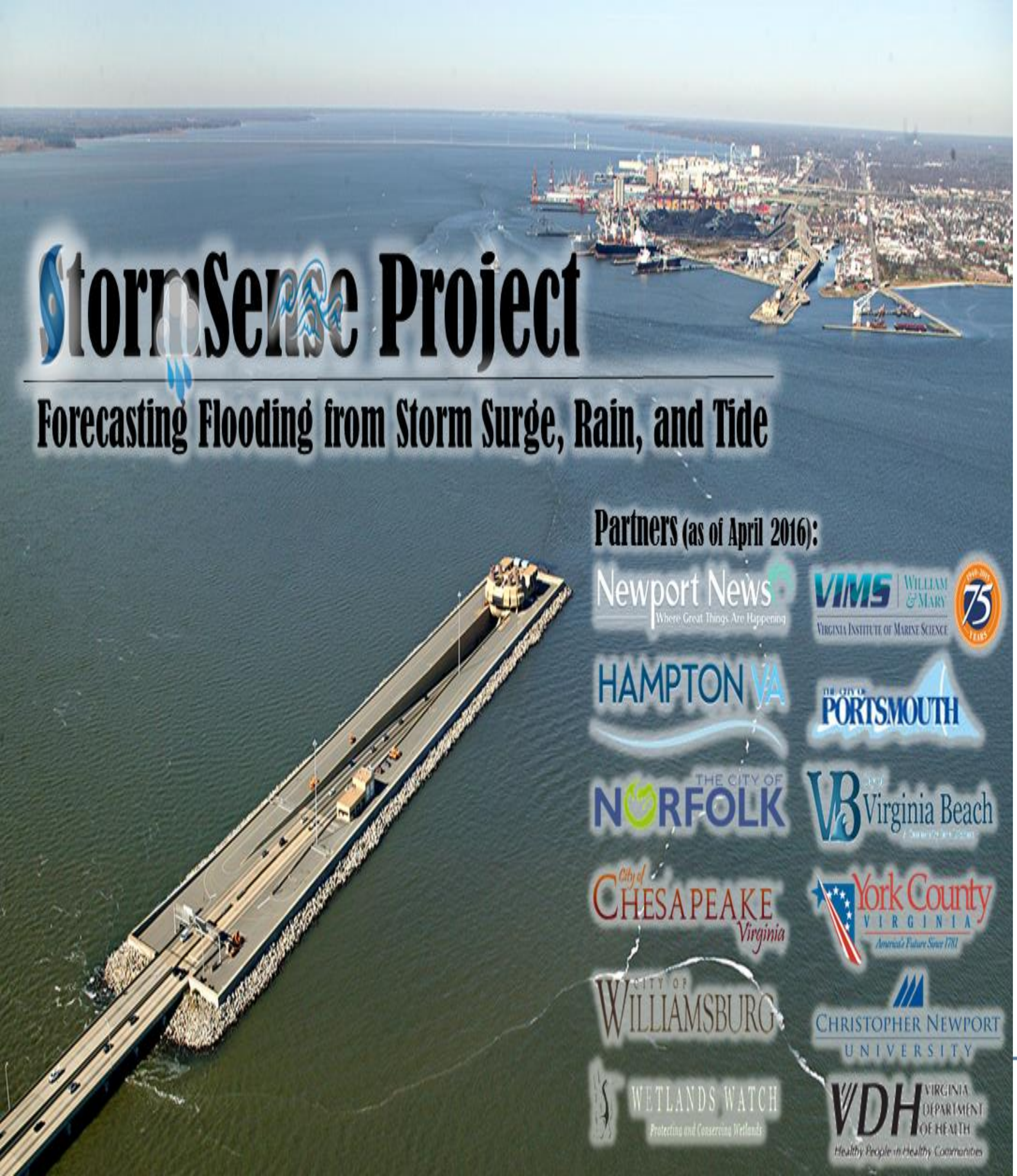
Bidirectional metering

Electric vehicles

Smart appliances

Ubiquitous networked sensors

Smart meters and real time usage data



StormSense Project

Forecasting Flooding from Storm Surge, Rain, and Tide

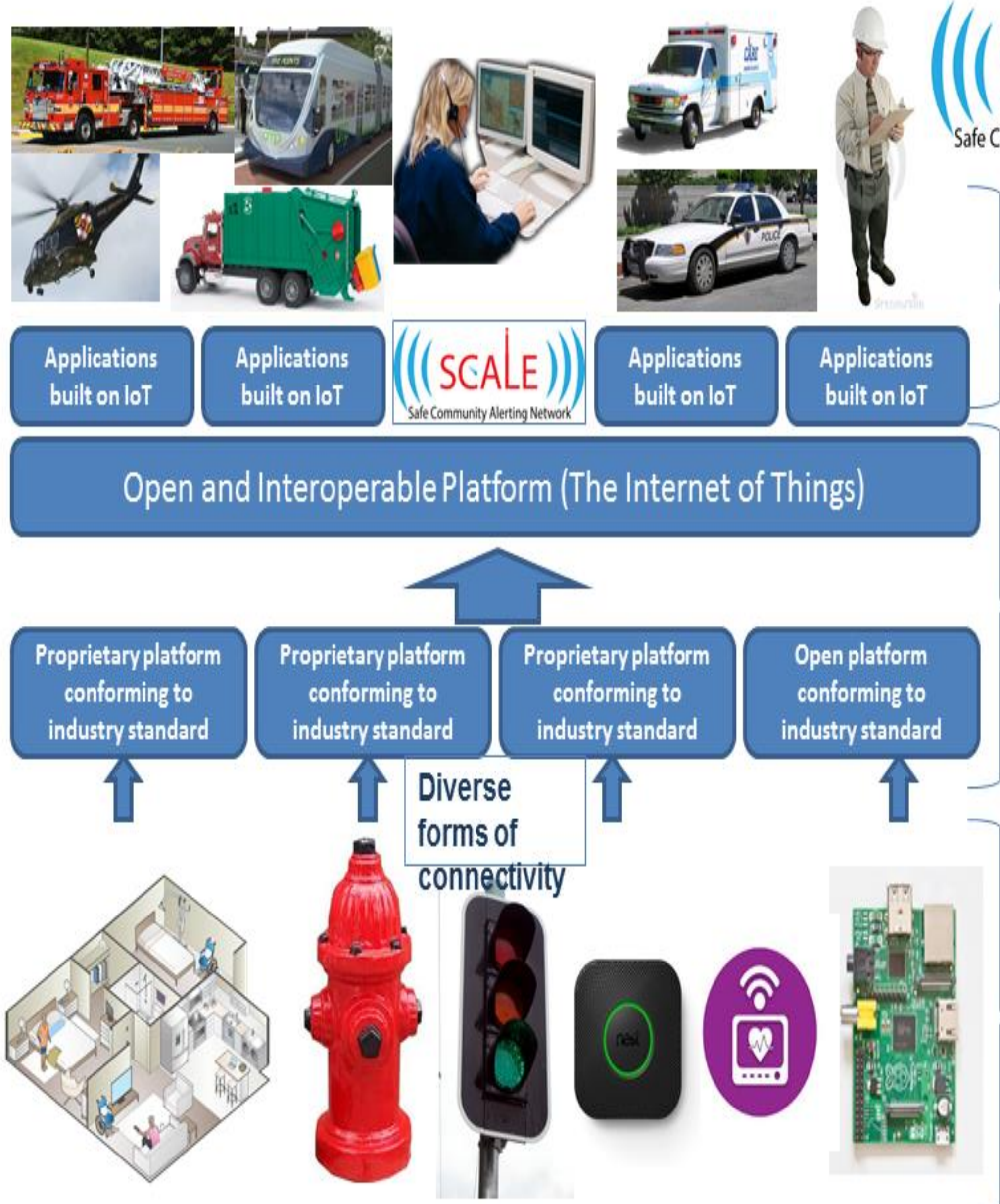
Partners (as of April 2016):

Newport News
Where Great Things Are Happening
VIMS William & Mary
Virginia Institute of Marine Science
75 Years
Hampton VA
The City of Portsmouth
The City of Norfolk
VB Virginia Beach
City of Chesapeake Virginia
York County Virginia
America's Future Since 1781
City of Williamsburg
Christopher Newport University
Wetlands Watch
Protecting and Conserving Wetlands
VDH Virginia Department of Health
Healthy People in Healthy Communities

SCALE

Safe Community Alerting Network

Phase Two



Applications built on IoT
Applications built on IoT
SCALE
Safe Community Alerting Network
Applications built on IoT
Applications built on IoT
Open and Interoperable Platform (The Internet of Things)
Proprietary platform conforming to industry standard
Proprietary platform conforming to industry standard
Proprietary platform conforming to industry standard
Open platform conforming to industry standard
Diverse forms of connectivity

Public Sector Apps built on the IoT.

Identify existing open standards and protocols that will allow varying devices to share their data securely.

A diverse ecosystem of IoT products make up a real world test bed. Many use cases will be demonstrated.

University of California-Irvine, Massachusetts Institutes of Technology, IBM, Intel, AT&T, SigFox, Brivo Labs, Senseware, N5 Sensors, the Telemedicine and Advanced Technology Research Center (TATRC), Responder, Del Ray Analytics, biobright, EIC Data, IoT DC, Captiva, Earth Networks, Victory Housing and more to come

Managing Cybersecurity Risks

“The growing convergence, interconnectedness, interdependence, and global nature of cyber and physical systems means that cybersecurity must be better managed in all contexts—international, national, organizational, and individual.”

-- *Report on Securing and Growing the Digital Economy*, Commission on Enhancing National Cybersecurity, 12/1/2016

Risks in the context of Smart Cities

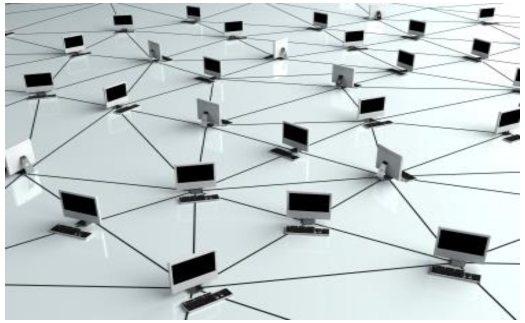
- Cybersecurity
  - Greater dependence on IT infrastructure
  - More systems connected
  - Systems working without a human in the loop

- Privacy
  - Significant amount of behavioral data
  - Large data stores will be created

The Challenge of Cybersecurity in Smart Cities

- Greater Automation Can Impact Resilience
  - Lack of manual operation mode
  - Problems may propagate faster than they can be fixed
  - Can launch attacks on multiple fronts with little effort

- Larger Attack Surface



- Incentives may increase

The Challenge of Cybersecurity in Smart Cities

- Development by silo can lead to cybersecurity challenges

  - Lack of Interoperability
    - Connecting systems that previously were unconnected
    - These are industries that have no communication with each other

  - Inconsistency in Cybersecurity
    - Industries and sectors that were entirely separate are now connected
    - Tradition of each industry ‘building its own’
    - Different industries will have different levels of cybersecurity expertise
    - An attacker will go for the weakest point and only needs one way in

HOW DO YOU APPROACH THIS?

A Risk-Based Approach

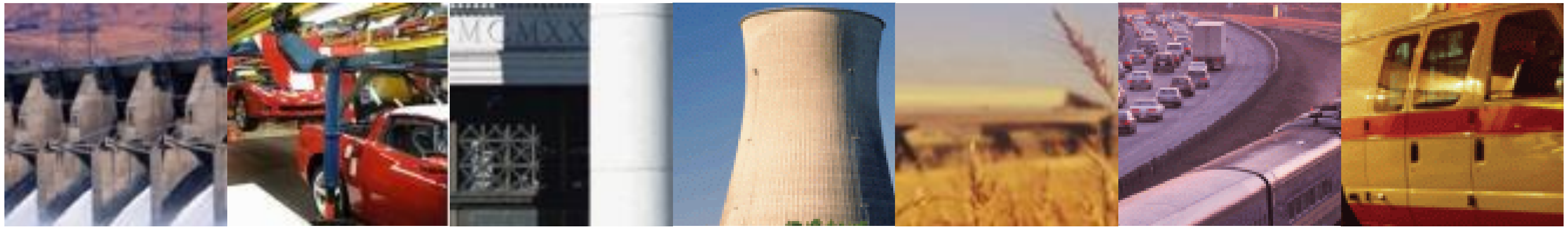
Need an approach that allows all of the different stakeholders (government, industry, non-profits and individuals) to have an understanding of cybersecurity objectives.

- Understand the risks in the context of missions
- Understand and communicate of the level of cybersecurity needed and achieved
- Understand the level of cybersecurity offered by other participants

The Cybersecurity Framework

- The Cybersecurity Framework provides a methodology to understand and manage cybersecurity risks across organizations, industries and sectors
- It does this by:
  - Facilitating consistent set of business objectives across all participants
  - Creating a common understanding of risk
  - Allowing that understood risk to be translated into action
  - Providing a way to hold multiple parties to a common approach

The Cybersecurity Framework Is for Organizations…



- Of any size, in any sector in the critical infrastructure
- That already have a mature cyber risk management and cybersecurity program
- That don’t yet have a cyber risk management or cybersecurity program
- With a mission of helping keep up-to-date on managing risk and facing business or societal threats

Taxonomy Value Proposition

Plant classification is the placing of known plants into groups or categories to show some relationship. Scientific classification follows a system of rules that standardizes the results, and groups successive categories into a hierarchy.

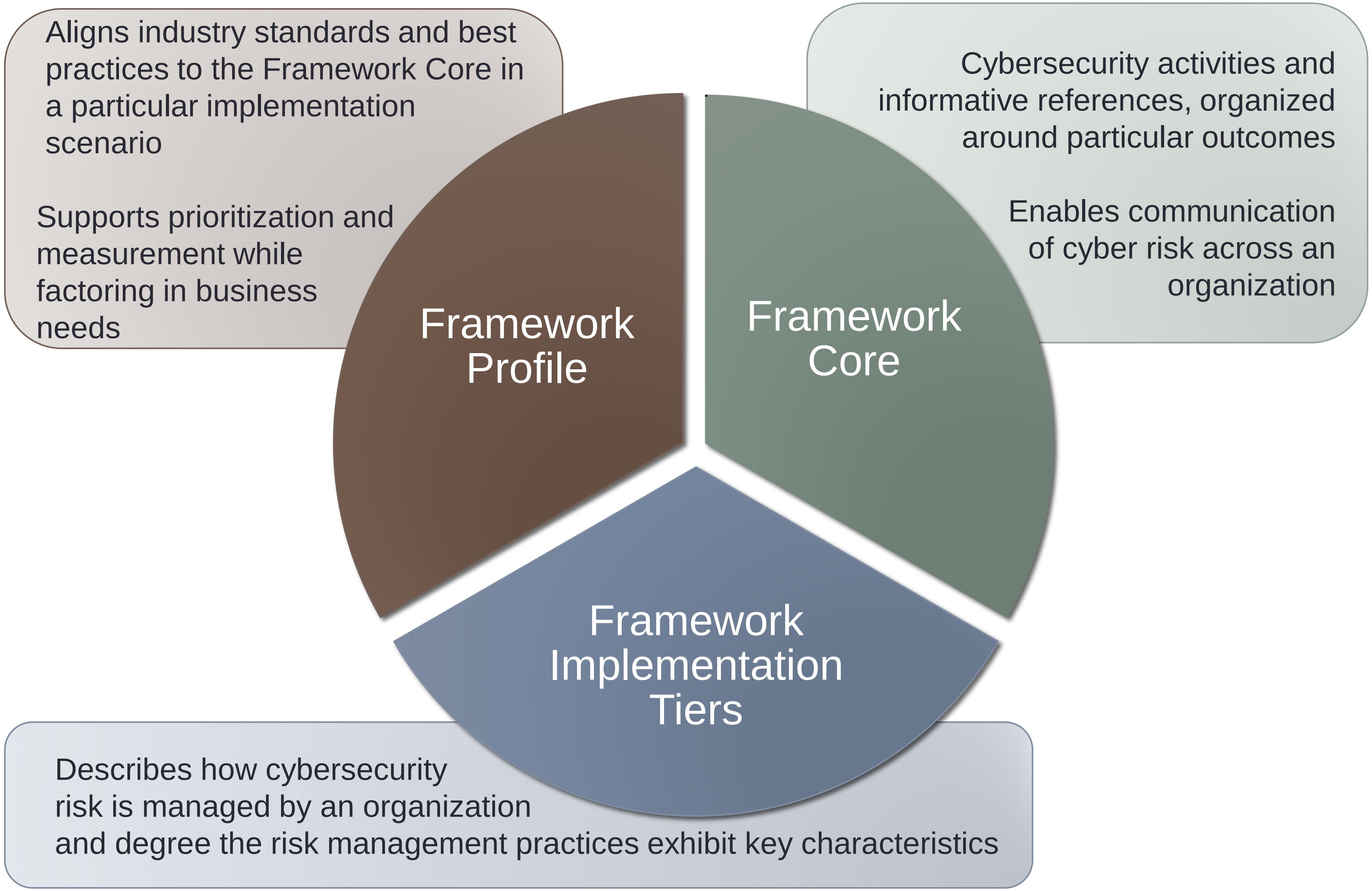
For example, the family to which lilies belong is classified as:

- **Kingdom:** Plantae
- **Phylum:** Magnoliophyta
- **Class:** Liliopsida
- **Order:** Liliales
- **Family:** Liliaceae
- **Genus:** ......
- **Species:** ......

Value Proposition

- Accurate communication
- Quickly categorize known
- Logically name unknown
- Inherent properties understood based on name

Framework Components



Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs

Framework Profile

Framework Core

Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Framework Implementation Tiers

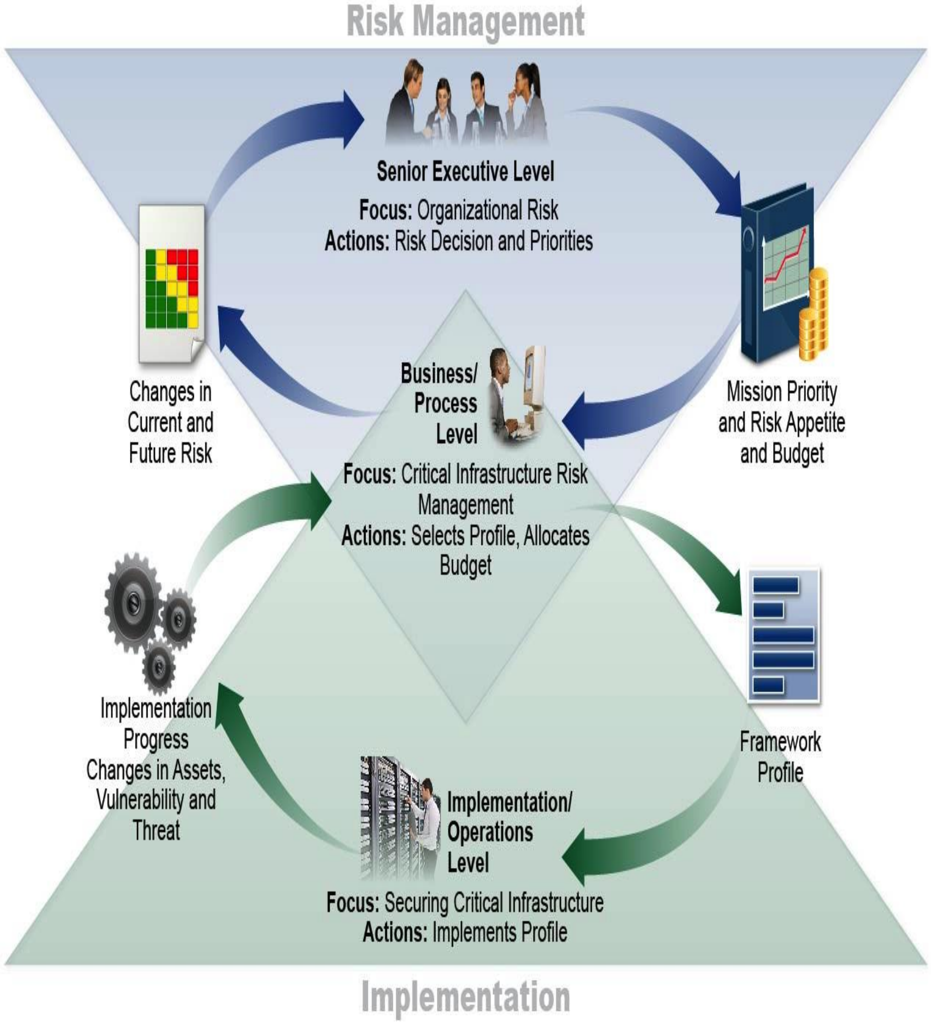
Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Applies within and among organizations

- A tool that provides organizations of all types, sizes, and capabilities with a common language for understanding, expressing and managing cybersecurity risks

- Facilitates communication within and across organizations, and at all levels of the organization

- A Framework (not a silver bullet)



Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profile
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

How is it being used today?

More Information

- On the Cybersecurity Framework
  - http://www.nist.gov/cyberframework
  - Email: cyberframework@nist.gov

- On Smart Cities
  - www.globalcityteams.org

- NIST GCTC
  - https://www.nist.gov/el/cyber-physical-systems/smart-americaglobal-cities

Questions?