

Cybersecurity Framework Overview

Implementation of Executive Order 13636
December 16, 2014

Kevin Stine
Kevin.Stine@nist.gov



National Institute of Standards and Technology (NIST)

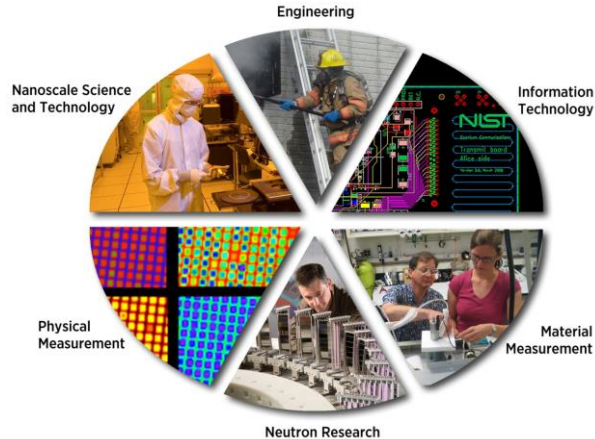
About NIST

- **Part of the U.S. Department of Commerce**
- **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**

Computer Security Division



The Computer Security Division provides standards and guidelines, tools, metrics, and practices to protect information and information systems.

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

Executive Order: Improving Critical Infrastructure Cybersecurity

“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”

President Barack Obama

Executive Order 13636, Feb. 12, 2013

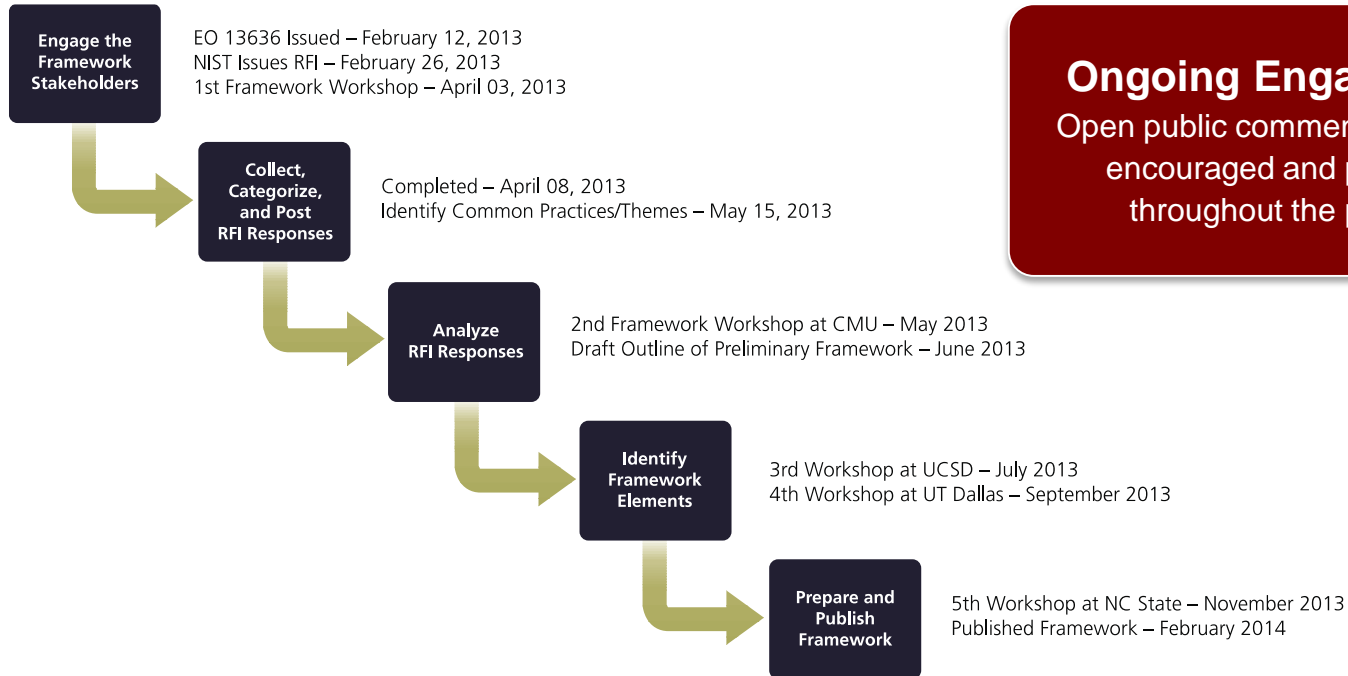
- The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a **voluntary framework for reducing cyber risks to critical infrastructure**
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a **roadmap for future work**



Based on the Executive Order, the Cybersecurity Framework Must...

- Include a set of standards, methodologies, procedures, and processes that **align policy, business, and technological approaches to address cyber risks**
- Provide a **prioritized, flexible, repeatable, performance-based, and cost-effective approach**, including information security measures and controls, to help owners and operators of critical infrastructure **identify, assess, and manage cyber risk**
- **Identify areas for improvement** to be addressed through future collaboration with particular sectors and standards-developing organizations
- **Be consistent with voluntary international standards**

Development of the Framework

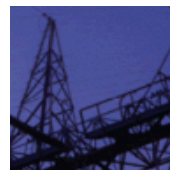
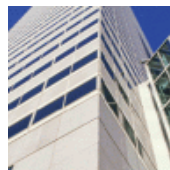
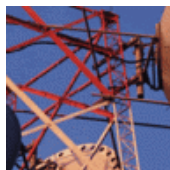


Ongoing Engagement:
Open public comment and review encouraged and promoted throughout the process

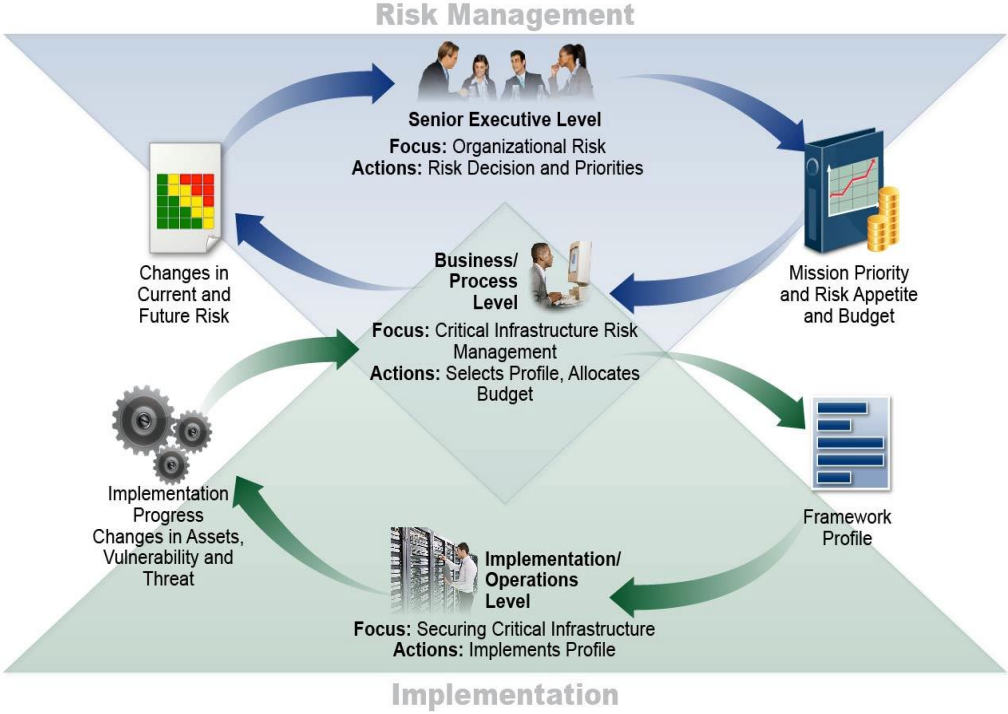
The Cybersecurity Framework Is for Organizations...



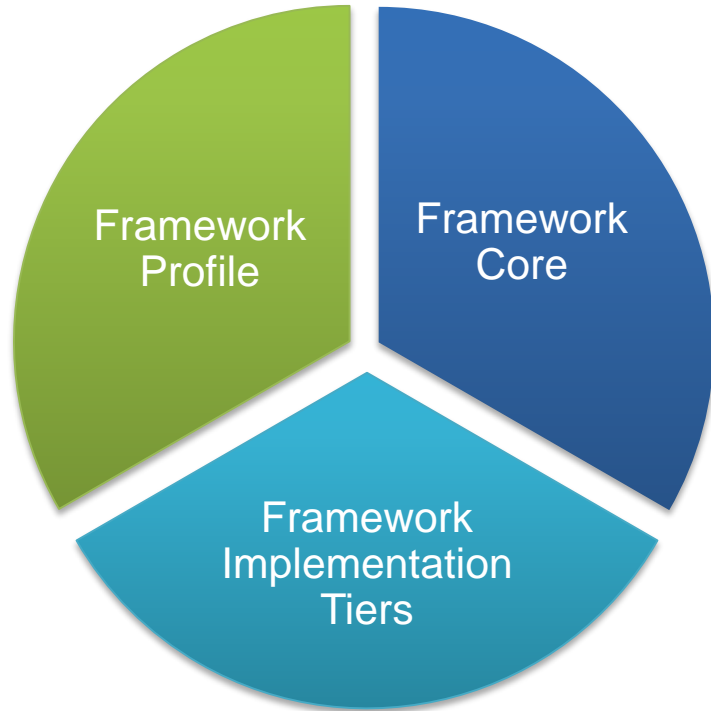
- Of **any size**, in **any sector** in the critical infrastructure
- That already have a **mature** cyber risk management and cybersecurity program
- That **don't yet** have a cyber risk management or cybersecurity program
- With a mission of **helping keep up-to-date** on managing risk and facing business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



Must Apply from Executives to Operations



Framework Components



Framework Profile

- 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 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

Framework Core

What assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

Function	Categories	Subcategories	References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

How to Use the Cybersecurity Framework

The Framework is designed to **complement existing business and cybersecurity operations**, and can be used to:

- Understand security status
- **Establish / Improve a cybersecurity program**
- Communicate cybersecurity requirements with stakeholders, including partners and suppliers
- Identify opportunities for new or revised standards
- Identify tools and technologies to help organizations use the Framework
- Integrate privacy and civil liberties considerations into a cybersecurity program

What's Next: Areas for Development, Alignment, and Collaboration

- The Executive Order calls for the framework to “identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations”
- **High-priority areas for development, alignment, and collaboration** were identified based on stakeholder input:
 - Authentication
 - Automated Indicator Sharing
 - Conformity Assessment
 - Cybersecurity Workforce
 - Data Analytics
 - Federal Agency Cybersecurity Alignment
 - International Aspects, Impacts, and Alignment
 - Supply Chain Risk Management
 - Technical Privacy Standards

What's Next: Using the Cybersecurity Framework

“A model of public-private cooperation, this Framework will help industry and Government strengthen the security and resiliency of our critical infrastructure.”

– President Obama, September 30, 2014

- **Organizations—led by their senior executives—are using the framework to improve their cybersecurity programs**
- **Industry groups, associations, and non-profits are playing key roles in assisting their members to understand and use the framework by:**
 - Building or mapping their sector’s specific standards, guidelines, and best practices to the framework
 - Developing and sharing examples.
- **The U.S. Government is committed to helping organizations understand and use the framework, getting feedback on initial use.**

Key Points about the Framework

- **It's a framework, not a prescription**
 - It provides a common language and systematic methodology for managing cyber risk
 - It does not tell a company *how* much cyber risk is tolerable, nor does it claim to provide “the one and only” formula for cybersecurity
 - Having a common lexicon to enable action across a very diverse set of stakeholders will enable the best practices of elite companies to become standard practices for everyone
- **The framework is a living document**
 - It is intended to be updated over time as stakeholders learn from implementation, and as technology and risks change
 - That's one reason why the framework focuses on questions an organization needs to ask itself to manage its risk. While practices, technology, and standards will change over time—principals will not

Where to Learn More and Stay Current

The *Framework for Improving Critical Infrastructure Cybersecurity*, the *Roadmap*, and related news and information are available at:

<http://www.nist.gov/cyberframework>

Email: cyberframework@nist.gov

Healthcare's Implementation of the NIST Cybersecurity Framework

Dr. Bryan Cline, CISSP-ISSEP, CISM, CISA, CCSFP, HCISPP
Senior HITRUST Advisor

Michael Frederick, CISSP, CCSFP
VP, Assurance Services & Product Development



Outline

- **Introduction**
- **Implementing the NIST Framework**
 - Addressing NIST Framework Objectives
 - Further Tailoring of the NIST Framework
- **How Organizations Can Get Started**
 - Per the NIST Framework
 - Additional HITRUST Recommendations
- **Q&A**



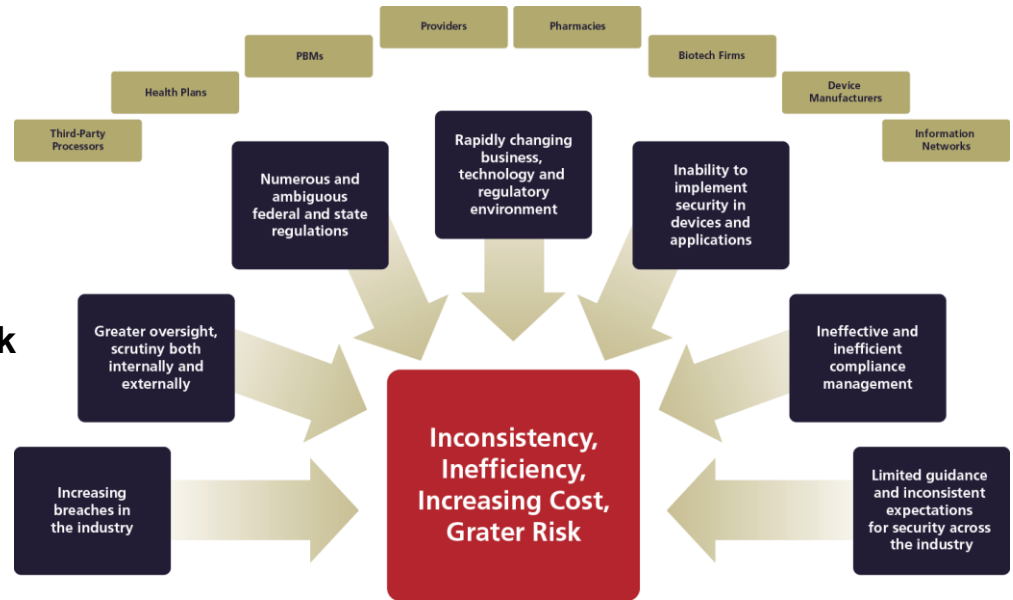
Introduction

- **Multitude of challenges**
 - Significant Oversight
 - Evolving requirements
 - Complex business relationships
 - Uncertain standard of care
 - Reasonable & appropriate?
 - Adequate protection?

- **HITRUST Risk Management Framework**

- Components include:
 - Common Security Framework (CSF™)
 - CSF Assurance Program
 - Related methods and tools, such as MyCSF™
- Standard of due care and diligence

- **HITRUST RMF = NIST Cybersecurity Framework PLUS ...**



Introduction

Dec 2011: GAO Report on Critical Infrastructure Protection

Apr 2012: HITRUST C3

Apr 2013: CSF Controls Relevant to Cybersecurity

Oct 2013: Preliminary Cybersecurity Framework

Mar 2014: Healthcare sector-wide Threat Intelligence Sharing (w/ HHS)

Apr/May 2014: 2014 CSF v6.1 formally incorporates NIST Cybersecurity Framework

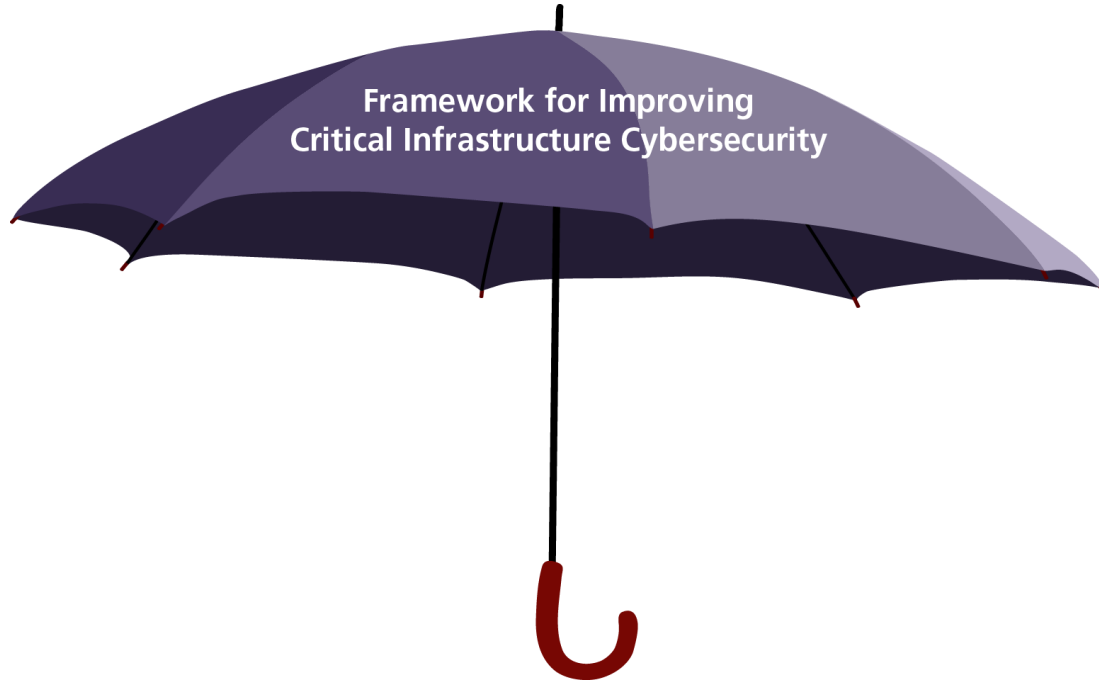
Feb 2013: President's E.O. 13636

Aug 2013: Discussion Draft, Preliminary Cybersecurity Framework

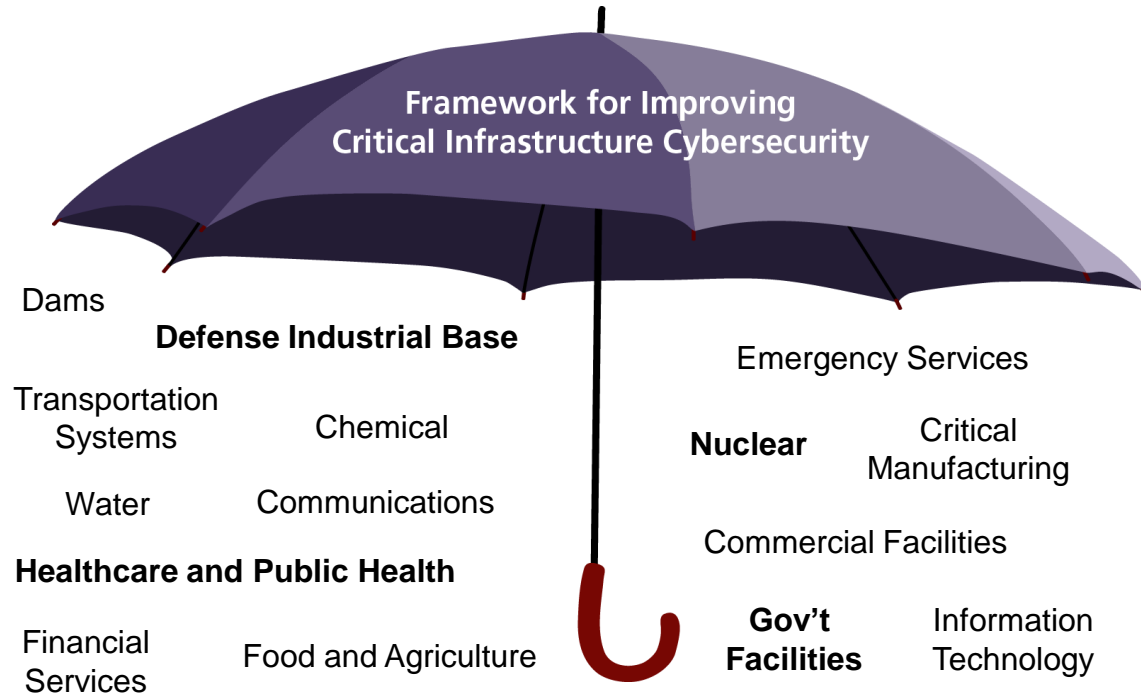
Feb 2014: Cybersecurity Framework (Final Release)

Apr 2014: CyberRX (w/ HHS)

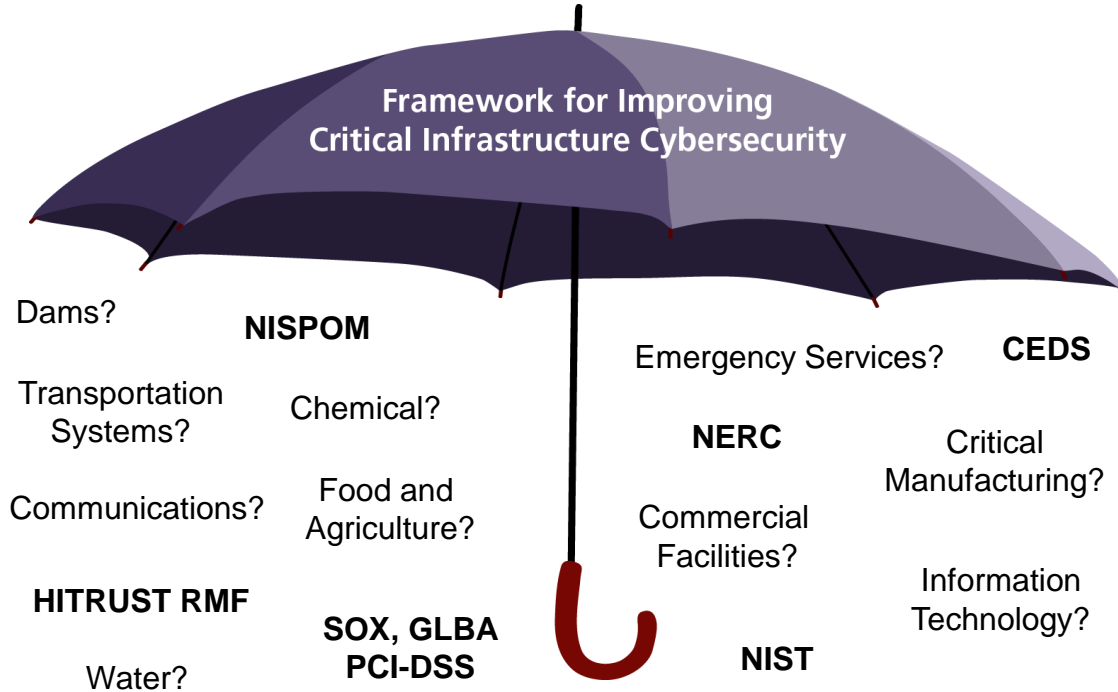
Implementing the NIST Framework



Implementing the NIST Framework



Implementing the NIST Framework



Implementing the NIST Framework

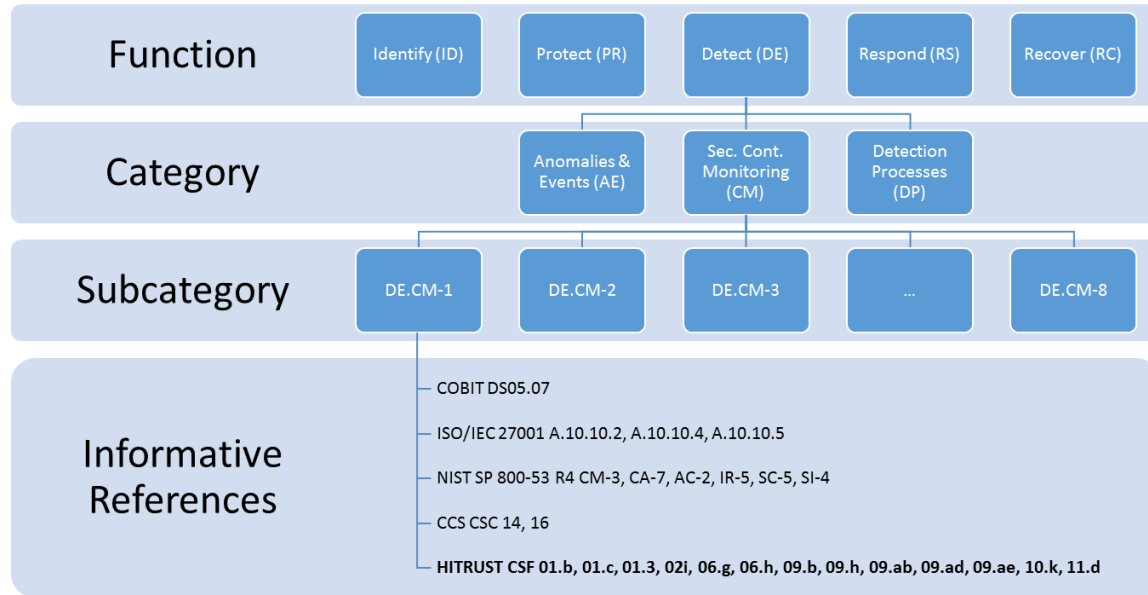


Addressing the NIST Framework Objectives

- 1. Describe target state for cybersecurity**
- 2. Describe current cybersecurity posture**
- 3. Identify and prioritize opportunities for improvement within the context of risk management**
- 4. Assess progress toward the target state**
- 5. Foster communications among internal and external stakeholders**

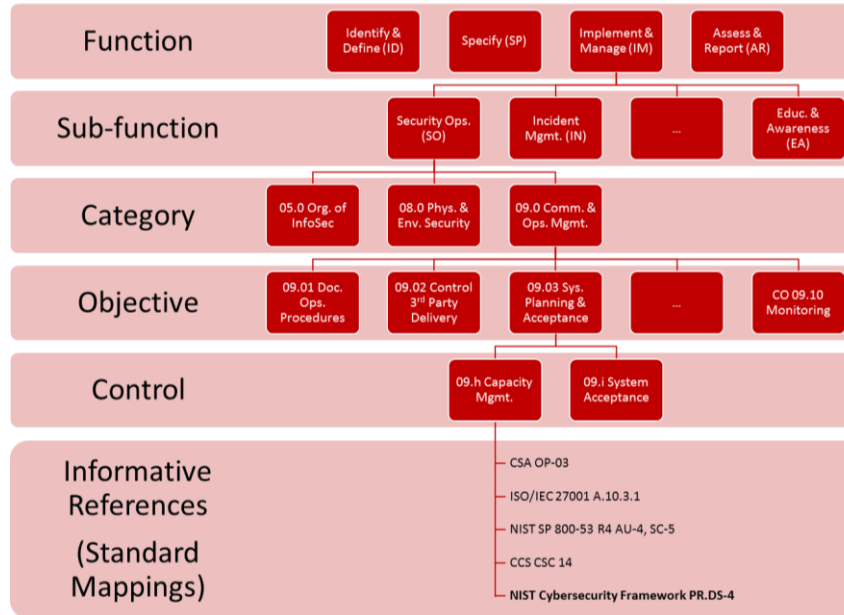
Addressing the NIST Framework Objectives

1. Describe target state for cybersecurity

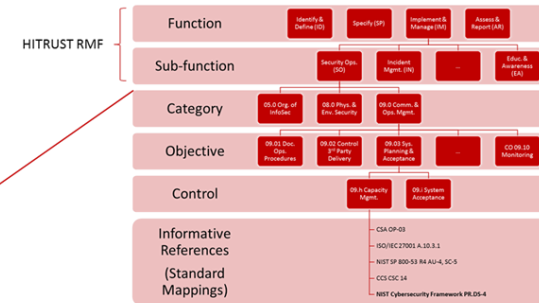
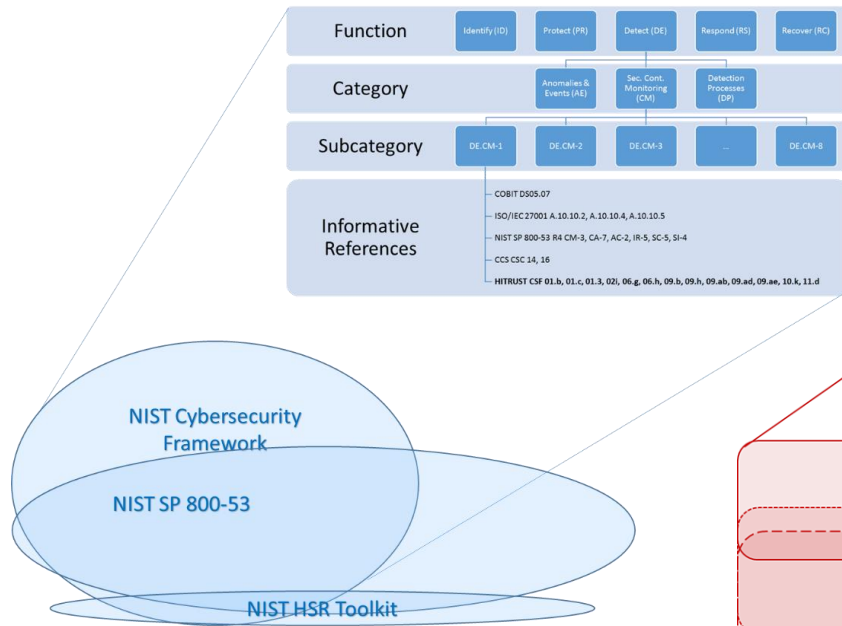


Addressing the NIST Framework Objectives

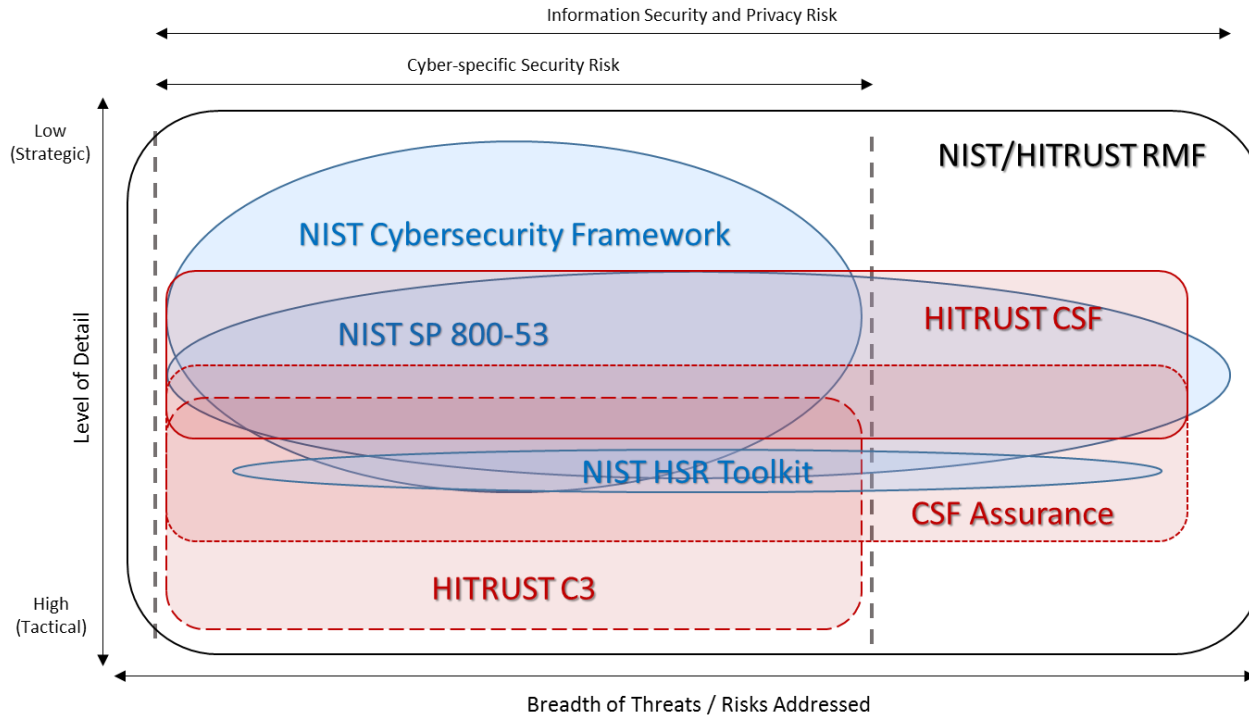
1. Describe target state for cybersecurity



Addressing the NIST Framework Objectives



Addressing the NIST Framework Objectives



Addressing the NIST Framework Objectives

1. Describe target state for cybersecurity

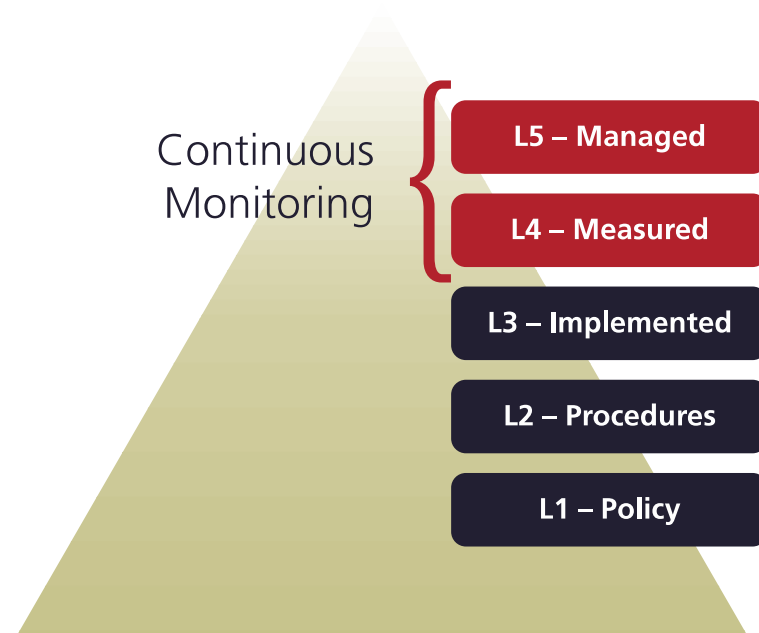
- **Three risk-based control baselines**
 - Organizational type and size
 - System requirements
 - Regulatory requirements
- **Additional tailoring encouraged**
 - Alternate controls: one-time or general use
 - Currently developing additional guidance for risk analysis

01.0 - Access Control	02.0 - Human Resources Security	03.0 - Risk Management	04.0 - Security Policy
01.a, 01.b, 01.c, 01.d, 01.e, 01.f, 01.g, 01.h, 01.i, 01.j, 01.k, 01.l, 01.m, 01.n, 01.o, 01.p, 01.q, 01.r, 01.s, 01.t, 01.u, 01.v, 01.w, 01.x, 01.y, 01.z	02.a, 02.b, 02.c, 02.d, 02.e, 02.f, 02.g, 02.h, 02.i, 02.j, 02.k, 02.l, 02.m, 02.n, 02.o, 02.p, 02.q, 02.r, 02.s, 02.t, 02.u, 02.v, 02.w, 02.x, 02.y, 02.z	03.a, 03.b, 03.c, 03.d, 03.e, 03.f, 03.g, 03.h, 03.i, 03.j, 03.k, 03.l, 03.m, 03.n, 03.o, 03.p, 03.q, 03.r, 03.s, 03.t, 03.u, 03.v, 03.w, 03.x, 03.y, 03.z	04.a, 04.b, 04.c, 04.d, 04.e, 04.f, 04.g, 04.h, 04.i, 04.j, 04.k, 04.l, 04.m, 04.n, 04.o, 04.p, 04.q, 04.r, 04.s, 04.t, 04.u, 04.v, 04.w, 04.x, 04.y, 04.z
05.0 - Organization of Information Security	06.0 - Compliance	07.0 - Asset Management	08.0 - Physical and Environmental Security
05.a, 05.b, 05.c, 05.d, 05.e, 05.f, 05.g, 05.h, 05.i, 05.j, 05.k, 05.l, 05.m, 05.n, 05.o, 05.p, 05.q, 05.r, 05.s, 05.t, 05.u, 05.v, 05.w, 05.x, 05.y, 05.z	06.a, 06.b, 06.c, 06.d, 06.e, 06.f, 06.g, 06.h, 06.i, 06.j, 06.k, 06.l, 06.m, 06.n, 06.o, 06.p, 06.q, 06.r, 06.s, 06.t, 06.u, 06.v, 06.w, 06.x, 06.y, 06.z	07.a, 07.b, 07.c, 07.d, 07.e, 07.f, 07.g, 07.h, 07.i, 07.j, 07.k, 07.l, 07.m, 07.n, 07.o, 07.p, 07.q, 07.r, 07.s, 07.t, 07.u, 07.v, 07.w, 07.x, 07.y, 07.z	08.a, 08.b, 08.c, 08.d, 08.e, 08.f, 08.g, 08.h, 08.i, 08.j, 08.k, 08.l, 08.m, 08.n, 08.o, 08.p, 08.q, 08.r, 08.s, 08.t, 08.u, 08.v, 08.w, 08.x, 08.y, 08.z
09.0 - Communications and Operations Management	10.0 - Information Systems Acquisition, Development, and Maintenance	11.0 - Information Security Incident Management	12.0 - Business Continuity Management
09.a, 09.b, 09.c, 09.d, 09.e, 09.f, 09.g, 09.h, 09.i, 09.j, 09.k, 09.l, 09.m, 09.n, 09.o, 09.p, 09.q, 09.r, 09.s, 09.t, 09.u, 09.v, 09.w, 09.x, 09.y, 09.z	10.a, 10.b, 10.c, 10.d, 10.e, 10.f, 10.g, 10.h, 10.i, 10.j, 10.k, 10.l, 10.m, 10.n, 10.o, 10.p, 10.q, 10.r, 10.s, 10.t, 10.u, 10.v, 10.w, 10.x, 10.y, 10.z	11.a, 11.b, 11.c, 11.d, 11.e, 11.f, 11.g, 11.h, 11.i, 11.j, 11.k, 11.l, 11.m, 11.n, 11.o, 11.p, 11.q, 11.r, 11.s, 11.t, 11.u, 11.v, 11.w, 11.x, 11.y, 11.z	12.a, 12.b, 12.c, 12.d, 12.e, 12.f, 12.g, 12.h, 12.i, 12.j, 12.k, 12.l, 12.m, 12.n, 12.o, 12.p, 12.q, 12.r, 12.s, 12.t, 12.u, 12.v, 12.w, 12.x, 12.y, 12.z

Addressing the NIST Framework Objectives

2. Describe current cybersecurity posture

- **CSF Assurance Program**
 - Cost-effective risk assessment
 - High-risk controls (data breach analysis)
 - HIPAA implementation requirements
 - Trained & certified assessor organizations
 - Readiness assessments
 - Remediation/implementation support
- **Defined assessment methodology**
 - PRISMA-based control maturity model supports “repeatable” likelihood estimates
 - Non-contextual impact ratings provide initial risk estimates for analysis



Addressing the NIST Framework Objectives

2. Describe current cybersecurity posture

- **MyCSF**

- GRC-based platform
- CSF controls
- Illustrative procedures
- Assessment scoping
- Workflow management for assessments and remediation
- Documentation repository for test plans, CAPs, and supporting documentation
- Dashboards and reporting
- Automated submission of assessments for HITRUST validation & certification



Addressing the NIST Framework Objectives

3. Identify & prioritize opportunities for improvement

- HITRUST provides actionable guidance for organizations conducting risk analysis, including the development and prioritization of **Corrective Action Plans (CAPs)**
 - Residual Risk
 - PRISMA-based maturity estimates (likelihood)
 - Relative Impact Codes
 - NIST-based Priority Codes



Addressing the NIST Framework Objectives

4. Assess progress toward the target state

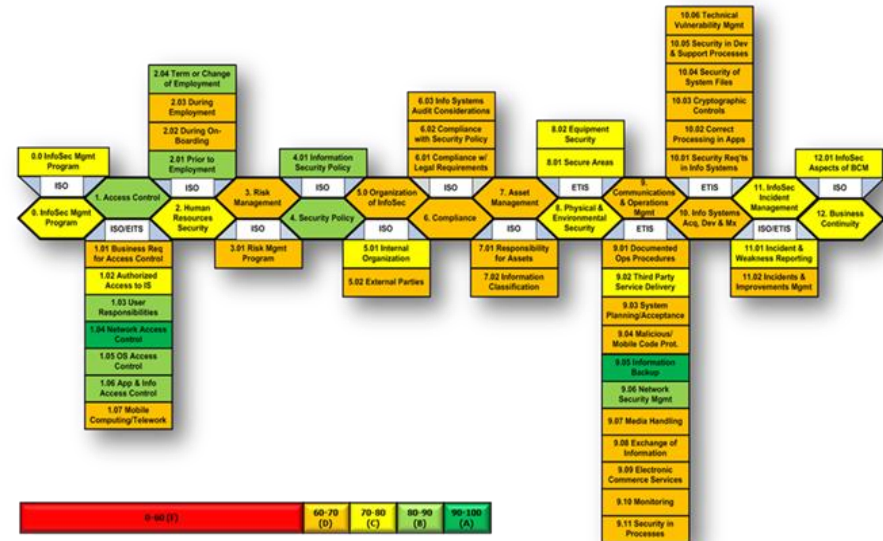
- The HITRUST CSF requires all organizations to develop CAPs and manage remediation activity
- HITRUST monitors remediation status for all CSF Certified organizations with outstanding CAPs
 - CSF requirements that score a 3 or below
 - Any requirement that is not fully implemented (i.e., not fully compliant for maturity level 3, Implemented).



Addressing the NIST Framework Objectives

5. Foster communication with stakeholders

- Standardized reporting supports third-party assurance for covered entities, business associates and regulators
- Maturity and risk calculations support internal baselines and external benchmarking



Addressing the NIST Framework Objectives

5. Foster communication with stakeholders

Cybersecurity Implementation Tiers	Cybersecurity Implementation Tier Description	Approximate HITRUST Maturity Levels	Approximate HITRUST Maturity Rating
Tier 0: Partial	Organization has not yet implemented a formal, threat-aware risk management process and may implement some portions of the framework on an irregular, case-by-case basis; may not have capability to share cybersecurity information internally and might not have processes in place to participate, coordinate or collaborate with other entities.	Level 1 – Partial Level 2 – Partial Level 3 – Partial Level 4 – Non-compliant Level 5 – Non-compliant	1 to 3-
Tier 1: Risk-Informed	Organization uses a formal, threat-aware risk management process to develop [target] profile [control requirements]; formal, approved processes and procedures are defined and implemented; adequate training & resources exist for cybersecurity; organization aware of role in “ecosystem” but has not formalized capabilities to interact/share info externally.	Level 1 – Partial Level 2 – Compliant Level 3 – Compliant Level 4 – Non-compliant Level 5 – Non-compliant	3- to 3+
Tier 2: Repeatable	Organization regularly updates [target] profile [control requirements] due to changing threats; risk-informed policies, processes and procedures are defined, implemented as intended, and validated; consistent methods are in place to provide updates when a risk change occurs; personnel have adequate skills & knowledge to perform tasks; organization understands dependencies/partners and can consume information from these partners.	Level 1 – Compliant Level 2 – Compliant Level 3 – Compliant Level 4 – Partial Level 5 – Partial	4- to 5-
Tier 3: Adaptive	Organization proactively updates [target] profile [control requirements] based on predictive indicators; actively adapts to changing/evolving cyber threats; risk-informed decisions are part of organizational culture; manages and actively shares information with partners to ensure accurate, current information is distributed and consumed to improve cybersecurity before an event occurs.	Level 1 – Compliant Level 2 – Compliant Level 3 – Compliant Level 4 – Compliant Level 5 – Compliant	5 to 5+

Further Tailoring of the NIST Framework

- **Additional focus areas include:**
 - Statutory and regulatory requirements
 - Threat environment
 - Privacy

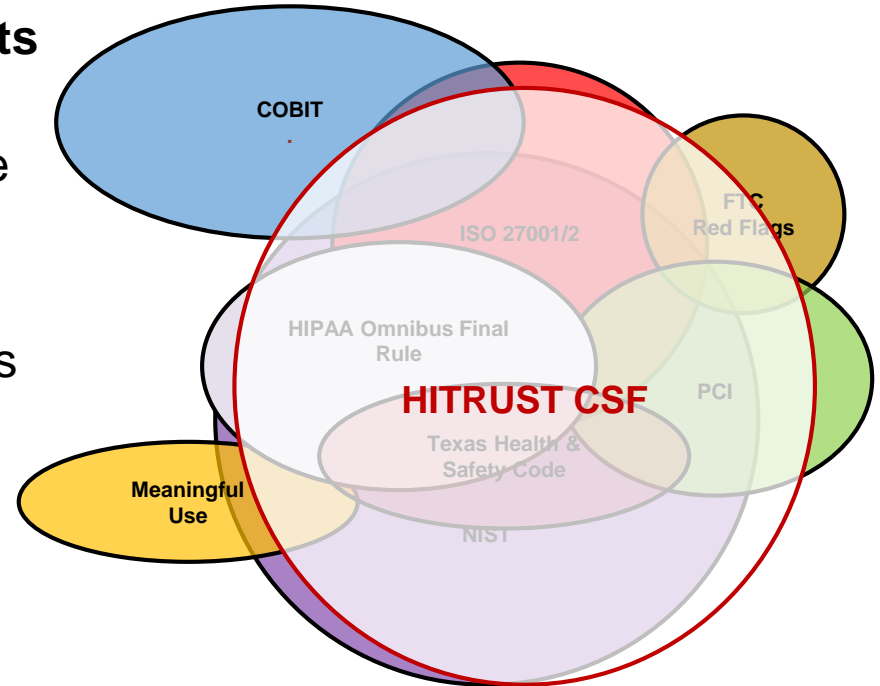


(from PwC's "[Why You Should Adopt the NIST Cybersecurity Framework](#)")

Further Tailoring of the NIST Framework

Statutory and regulatory requirements

- CSF rationalizes industry-relevant regulations & standards into a single overarching framework
- ISO provides the foundation
- NIST and other authoritative sources provides additional prescription



Further Tailoring of the NIST Framework

Threat environment

- Formally established in April 2012
- Result of growing threats posed by cyber attacks targeted at healthcare
- **HITRUST facilitates public-private collaboration**
 - Healthcare community
 - Department of Homeland Security
 - Department of Health and Human Services
- **Actionable intelligence specific to healthcare industry**
- <http://hitrustalliance.net/cyber-threat-intelligence/>
- <http://hitrustalliance.net/cyber-threat-briefings/>



Further Tailoring of the NIST Framework

Threat environment

- **New initiative to tie cyber threats to CSF**
 - Develop common threat taxonomy
 - Develop threat catalog for healthcare industry
 - Tie CSF controls to relevant threats
- **Better supports HIPAA requirements**
 - Address all reasonably anticipated threats; support risk analysis
- **Supports consumption of threat intelligence by organizations with various levels of cybersecurity program maturity**
 - Review status of controls based on current threat intelligence
 - Provide interim guidance between CSF releases
 - Update CSF requirements to better address threats



Further Tailoring of the NIST Framework

Threat environment

- Designed by an industry steering committee
- Participants included DHHS and multiple payers and providers
- Various scenarios including devices, systems, exchanges; Healthcare.gov
- Some key observations included:
 - Organizations varied in preparedness, ability to consume intel
 - Participation results in more preparedness
 - Gov't & HITRUST should explore additional info sharing and analysis
- **CyberRX 2.0 currently in planning stages**
- <http://hitrustalliance.net/cyberrx/>



Further Tailoring of the NIST Framework

Privacy

- **NIST Framework**
 - NIST SP 800-53 revision 4 Appendix J, Privacy Control Catalog
 - General privacy guidance from Preliminary Framework retained
- **HITRUST Framework**
 - Integrates HIPAA-based privacy controls
 - Limited to TX Covered Entity Privacy & Security Certification Program
 - Controls currently under revision by an industry working group
 - Will retain current structure and HIPAA focus
 - Will integrate NIST Privacy Control Catalog to support federal agencies
 - Will be made available to all HITRUST users
 - Will support general privacy certification program (TBD)

How Organizations Can Get Started

Per the NIST Framework

Cybersecurity Framework	HITRUST Framework
Step 1: Make Organization-wide Decisions	Adopt the HITRUST CSF
Step 2: Establish a Target Profile	Determine CSF control baseline using multiple risk-factors; identify alternate controls as needed
Step 3: Establish a Current Profile	Undergo a CSF assessment
Step 4: Compare Target and Current Profiles	Request CSF validated or certified report
Step 5: Implement Target Profile	Prioritize and implement corrective actions identified in the report


How Organizations Can Get Started

Additional HITRUST Recommendations

- **Integrate the HITRUST RMF into the Security Program**
 - Define Security Services (ref: ITIL)
 - Map Controls/Resources to Security Services
 - Develop Annual Work Plan to Address:
 - “Lights On” Work
 - Remediation Activity (Operational Work and Project Support, including Capital Budget Planning)
- **Keep the Security Program Relevant**
 - Integrate Threat Intelligence (e.g., HITRUST C3) Into Risk Management Processes
- **Develop/Improve/Exercise Incident Management Capabilities**
 - Internal Exercises
 - External (Multi-organizational) Exercises (e.g., CyberRX)


Questions?

Dr. Bryan Cline, CISSP-ISSEP, CISM, CISA, CCSFP, HCISPP

 (469) 269-1118

 Bryan.Cline@HITRUSTalliance.net

Michael Frederick, CISSP, CCSFP

 (469) 269-1205

 Michael.Frederick@HITRUSTalliance.net



About HITRUST

- **Born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges**
- **Led by a seasoned management team; governed by a Board of Directors made up of leaders from across the healthcare industry and its supporters**



- **More than seven years experience as the only industry-wide information protection standards and certification body in healthcare**
- **Driving adoption and widespread confidence in sound risk management practices through education, advocacy and other activities**

Question & Answer Session

