NIST Cybersecurity Framework

WaterISAC
July 22, 2014
Cheryl Santor, CGEIT, CISM, CISA, CISSP
Metropolitan Water District of So. CA

WaterISAC

Cheryl Santor, CGEIT, CISM, CISA, CISSP
Information Security Manager Metropolitan Water District

- 25 plus years as a security professional, yes, even before it was fashionable and necessary
- Information Security Program
- NERC/FERC delegate for Cyber Security at MWD
- NIST Cyber Security Framework delegate at MWD
- Member of ISACA 14 years – Past Los Angeles Chapter President
- Member of ISSA 14 years
- Member FBI Infragard 14 years

Presidential Order 13636

- February 12, 1013 – President Obama issues Presidential Order
- National Institute of Standards and Technology mandated to produce Cyber Security Framework
- Congress was ordered to provide supporting legislation for some areas: Information Sharing, Education in Cybersecurity, etc.
- One year later Cyber Security Framework issued

Order Directives

- Section 1, Policy – Improve the nation's cyber security due to repeated intrusions
- Section 2, Critical Infrastructure – Identify to reduce risk to security, national economy, national public health or safety
- Section 3, Policy Coordination – Leverage Presidential Directive of February 13, 2009
- Section 4, Cyber Security Information Sharing
- Section 5, Privacy and Civil Liberties Protections
- Section 6, Consultative Process – Use sector resources and public/private agencies, etc.

Order Directives (Continued)

- Section 7, Baseline Framework to Reduce Cyber Risk to Critical Infrastructure
- Section 8, **Voluntary** Critical Infrastructure Cybersecurity Program
- Section 9, Identification of Critical Infrastructure at Greatest Risk
- Section 10, Adoption of Framework
- Section 11, Definitions
- Section 12, Provisions

What Section of the Presidential Order Is Meaningful to Us?

- Section 7, The development of the NIST Cyber Security Framework
- One year to complete
- Draft presented for comments before final version published
- Living document; will undergo revisions as needed

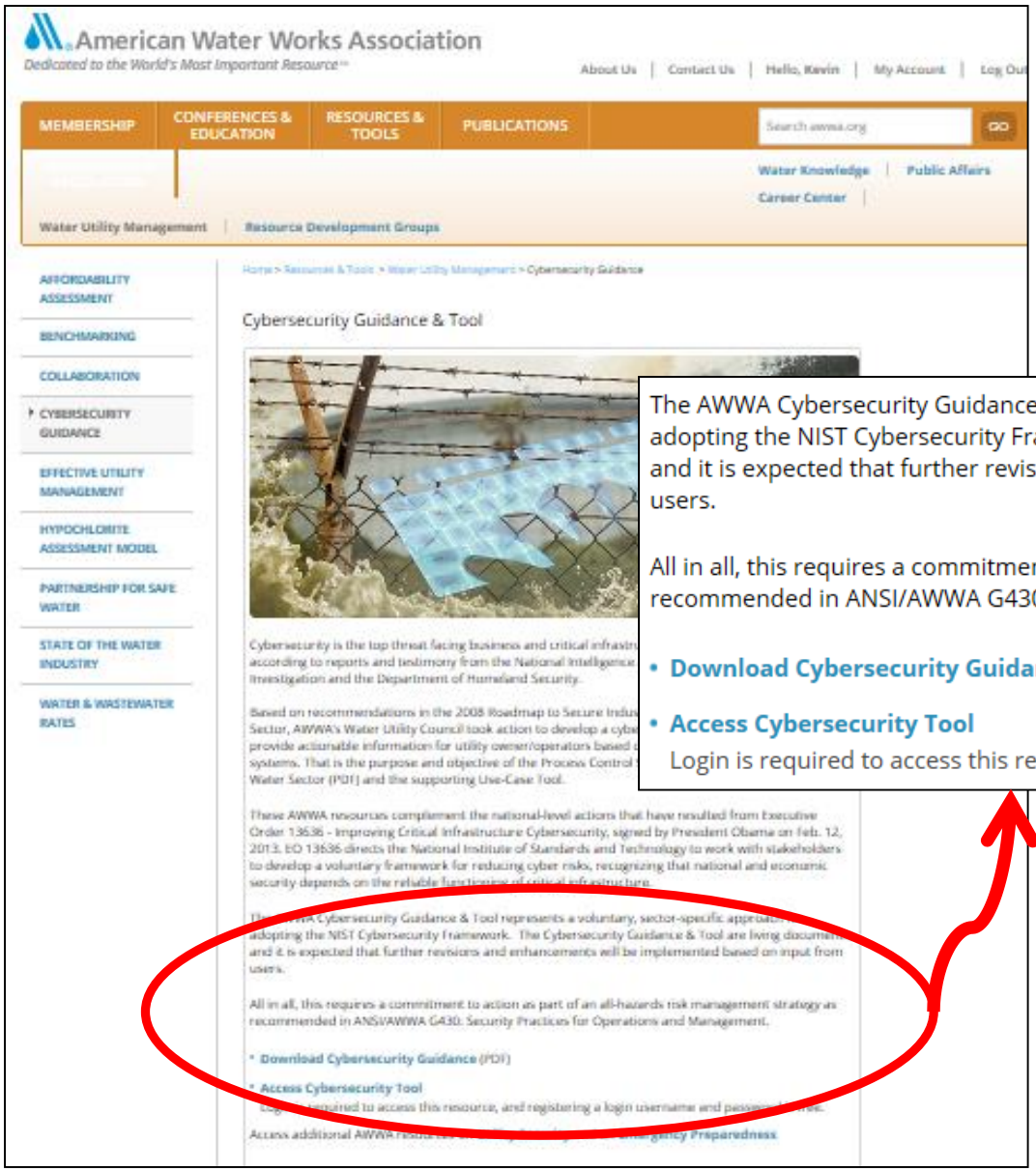
National Call to Action

Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013)

NIST Cybersecurity Framework (Feb 2014)

1. Framework Core
2. Framework Profile
3. Framework Implementation Tiers

Voluntary guidance to assist critical infrastructure and business's improve cybersecurity.



The AWWA Cybersecurity Guidance & Tool represents a voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework. The Cybersecurity Guidance & Tool are living documents, and it is expected that further revisions and enhancements will be implemented based on input from users.

All in all, this requires a commitment to action as part of an all-hazards risk management strategy as recommended in ANSI/AWWA G430: Security Practices for Operations and Management.

- **Download Cybersecurity Guidance** (PDF)
- **Access Cybersecurity Tool**
  Login is required to access this resource, and registering a login username and password is free.

WaterISAC

American Water Works Association

CYBERSECURITY REPORT

The following recommended cybersecurity controls represent measures the utility should consider to protect their Process Control System against cyber-attack. The controls have been assigned to four levels of priority based on the user's specific environment as defined by the use cases selected.

Priority 1 controls represent the minimum level of acceptable security for SCADA/PCS. If not already in place, these controls should be implemented immediately.

Priority 2 controls have the potential to provide a significant and immediate increase in the security of the organization.

Priority 3 controls provide additional security against cybersecurity attack of PCS Systems and lay the foundation for implementation of a managed security system. These controls should be implemented as soon as budget allows.

Priority 4 controls are more complex and provide protection for more sophisticated attacks (which are less common). Many Priority 4 controls are related to policies and procedures; others involve state-of-the-art protection mechanisms.

WaterISAC

Selected Use Cases:

Architecture

AR1: Dedicated network. All network and communications infrastructure is dedicated exclusively to SCADA. No connection to enterprise networks.

User Access

UA3: Remote system access with control. Access from location outside "control room" environment and located outside the physical perimeter of the facility.

Recommended Controls:

⊟ PRIORITY 1 CONTROLS

AU-2: Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.

DHS CAT: 2.1 Security Policy

ISO/IEC 27001-27005: Annex A: A.5 Security Policy

AU-3: Governance framework to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.

ISA 62443-2-1: 4.5 Management Responsibility

ISO/IEC 27001-27005: 27005 Whole Document

NIST 800-53: Appendix J: AR-1 Governance and Privacy Program

IA-10: Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.

DHS CAT: 12.15.11 Permitted Actions without ID or Authentication

Cybersecurity Framework

- DHS NIST conducted workshops across the country at universities to provide critical infrastructure opportunities to meet and discuss
- Draft Framework issued in October 2013 for critical infrastructure to review and make comments
- February 12, 2014 NIST Cybersecurity Framework issued
- NIST provided a Roadmap document to accompany the framework

Improving Critical Infrastructure Cybersecurity

- Policy – Partnership with the owners and operators of critical infrastructure to improve sharing and develop and implement risk-based standards.
- Critical Infrastructure – Systems and assets, physical or virtual, vital to the US that if destroyed or incapacitated would have debilitating impact on security, national economic security, national health or safety.

Overview of the Framework

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.

Framework Makeup

- The Framework ***Core*** is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.
  - Five concurrent and continuous Functions:
    - Identify
    - Protect
    - Detect
    - Respond
    - Recover

Framework Makeup (Continued)

- The Framework ***TIERS*** - How an organization views cybersecurity risk and the processes in place to manage that risk.
  - Tier 1: Partial
  - Tier 2: Risk Informed
  - Tier 3: Repeatable
  - Tier 4: Adaptive

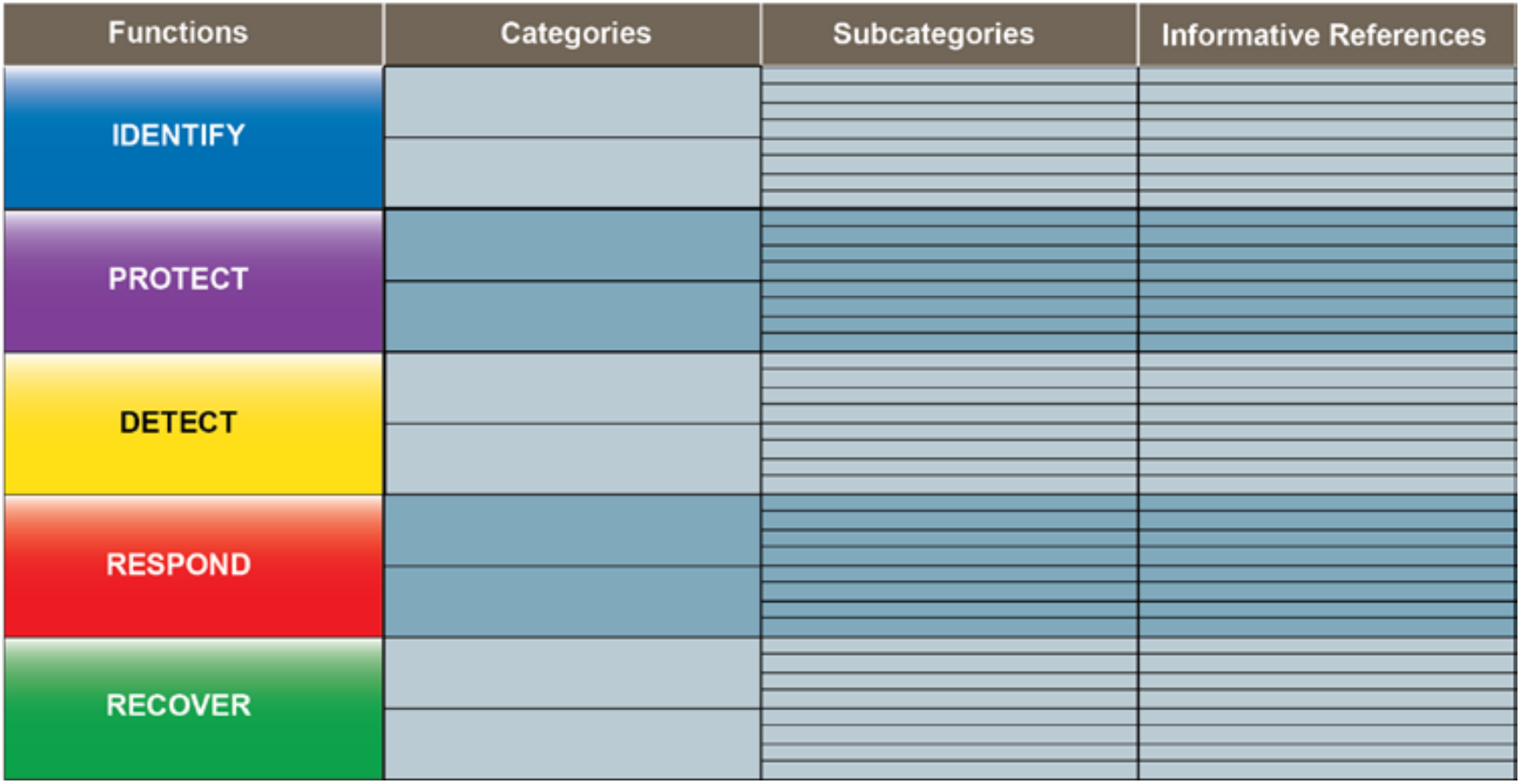
These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.

Framework Makeup (Continued)

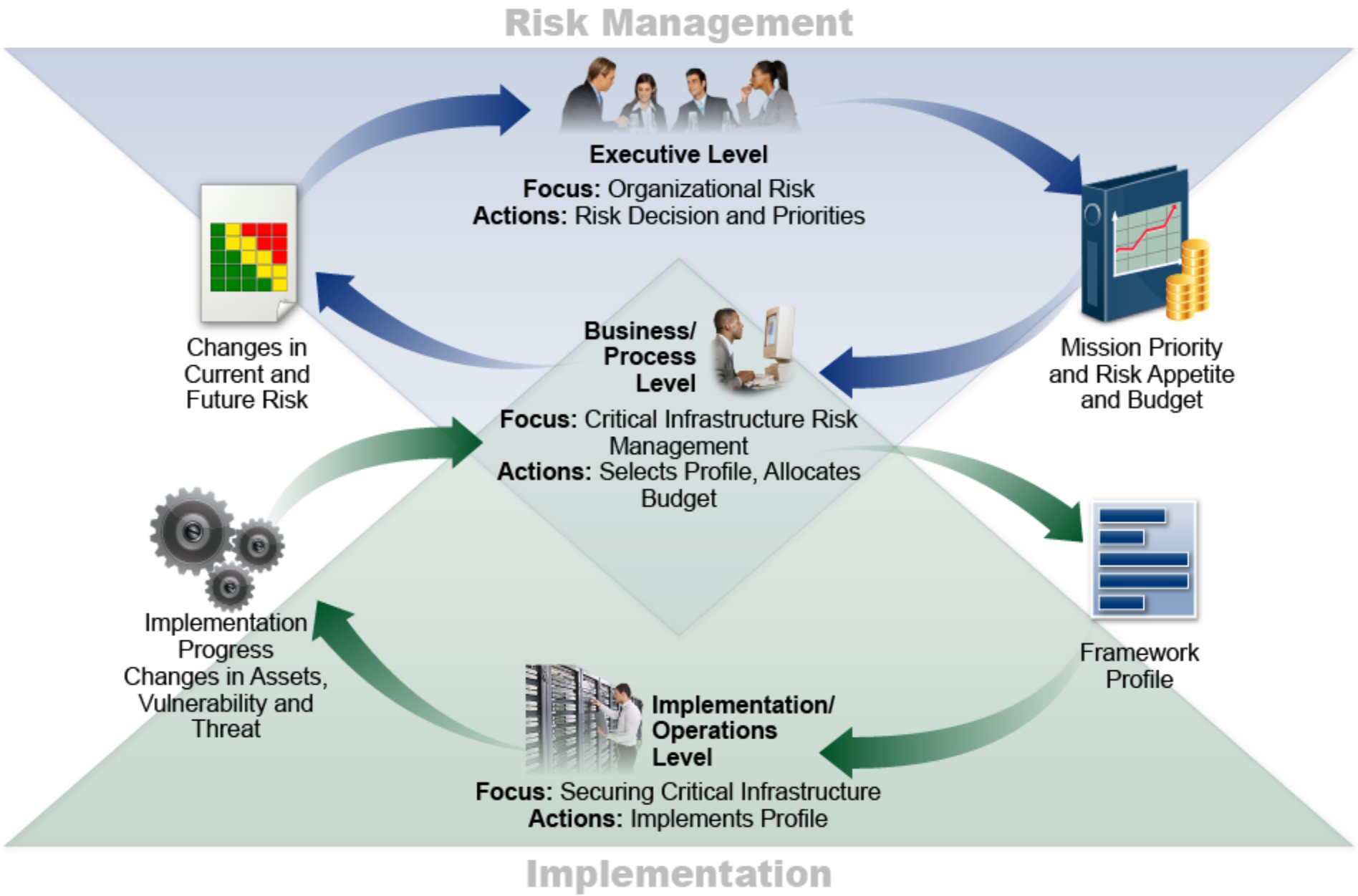
The Framework ***Profile*** - Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization.

- A Profile establishes a roadmap for reducing cybersecurity risk that is aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities.
- Framework Profiles describe the current state or the desired target state of specific cybersecurity activities, not prescriptive.
- Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives.

Framework Core Chart



Notional Information and Decision Flows within an Organization



How to Use the Framework

- Key part of systematic process to identify, assess, and manage cybersecurity
- Not designed to replace existing processes, can overlay those on Framework to determine gaps in risk approach and develop roadmap
- Risk management tool, determine activities most important and maximize investment
- Designed to complement existing business and cybersecurity operations
- Foundation for new cybersecurity program or to improve existing
- Expresses cybersecurity processes to partners and customers

Framework Core Chart

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Basic Review of Cybersecurity Practices

- Compare organizations current cybersecurity activities with those in Core
- Examine extent to which organization is achieving outcomes described in Core Categories and Subcategories
- Align with Identify, Protect, Detect, Respond, and Recover
- May already be achieving desired outcomes
- May determine opportunities to improve
- Use information to develop action plan to strengthen practices and reduce risk
- Reprioritize related to cost and risk
- Help to answer “How are we doing?” Move in more informed way

Establishing or Improving a Cybersecurity Program

- Steps how an organization could use the Framework to create a new cybersecurity program or improve an existing program:
  1. Prioritize and Scope
  2. Orient
  3. Create Current Profile
  4. Conduct a Risk Assessment *
  5. Create a Target Profile
  6. Determine, Analyze, and Prioritize Gaps
  7. Implement Action Plan

Communicating Cybersecurity Requirements with Stakeholders

- The Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure services. Examples include:
  - An organization may utilize a Target Profile to express cybersecurity risk management requirements to an external service provider (e.g., a cloud provider to which it is exporting data).
  - An organization may express its cybersecurity state through a Current Profile to report results or to compare with acquisition requirements.
  - A critical infrastructure owner/operator, having identified an external partner on whom that infrastructure depends, may use a Target Profile to convey required Categories and Subcategories.
  - A critical infrastructure sector may establish a Target Profile that can be used among its constituents as an initial baseline Profile to build their tailored Target Profiles.

Identify New Opportunities

The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization Might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices.

Privacy and Civil Liberties

- Executive order addresses individual privacy and civil liberties that may result from cybersecurity operations
- Framework intended as general set of considerations as different sectors may address processes with technical implementations
- Privacy standards, guidelines, and additional best practices may need to be developed
- Personal information used, collected, maintained, or disclosed in organizations' cybersecurity activities
- Example: over-collection, over-retention of PII, disclosure unrelated to activities or mitigation results in DOS

Governance of Cybersecurity Risk

- An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements
- Process is in place to assess implementation of the foregoing organizational measures and controls

Steps in Governance Activities

- Approaches to identifying and authorizing individuals to access organizational assets and systems
- Awareness and training measures
- Anomalous activity detection and system and assets monitoring
- Response activities, including information sharing or other mitigation efforts

DHS Critical Infrastructure Program

The Department of Homeland Security's Critical Infrastructure Cyber Community C³ Voluntary Program helps align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks. Learn more about the C³ Voluntary Program by visiting: www.dhs.gov/ccubedvp.

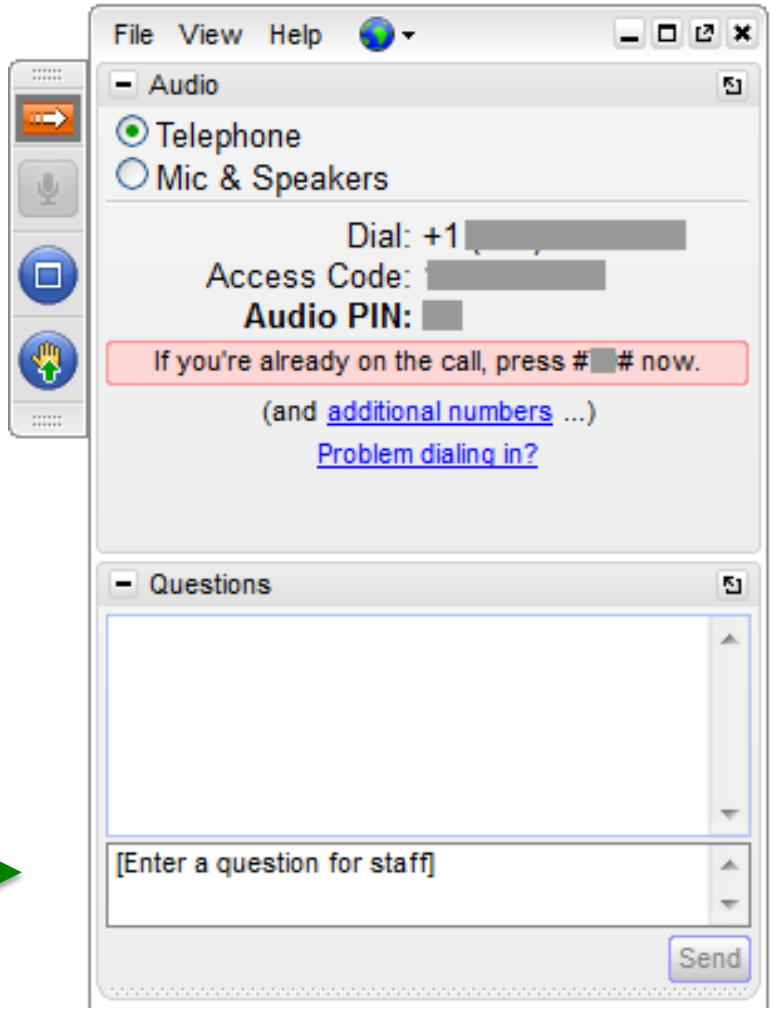
NIST Roadmap

NIST is also pleased to issue a companion Roadmap that discusses NIST's next steps with the Framework and identifies key areas of cybersecurity development, alignment, and collaboration. In the interest of continuous improvement, NIST will continue to receive and consider informal feedback about the Framework and Roadmap. As has been the case throughout the process, organizations and individuals may contribute observations, suggestions, and lessons learned to cyberframework@nist.gov

Cybersecurity Framework Roles & Responsibilities - MWD

Function	Category	Subcategory	Informative References	Area of Responsibility	Status and Comments	Cost/Estimate	Regulatory Requirement
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8	•	•	•	•
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8	•	•	•	•
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8	•	•	•	•
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9	•	•	•	•
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1	•	•	•	•

Questions?



Type and send

Thank You

WaterISAC Contact Information:

1-866-H2O-ISAC

Charles Egli
Lead Analyst
egli@waterisac.org

Michael Arceneaux
Managing Director
arceneaux@waterisac.org

Cheryl Santor, CGEIT, CISM, CISA, CISSP
Information Security Manager
Metropolitan Water District
of Southern California
csantor@mwdh2o.com

WaterISAC