
# CONCEPTS IN CYBER SECURITY

GARY KNEELAND, CISSP

SENIOR CONSULTANT

CRITICAL INFRASTRUCTURE & SECURITY PRACTICE

# OBJECTIVES

- FRAMEWORK FOR CYBERSECURITY
- CYBERSECURITY FUNCTIONS
- CYBERSECURITY CONTROLS
  - COMPARATIVE EXAMPLES
- REFERENCES

# US CRITICAL INFRASTRUCTURE


Chemical Sector


Defense Industrial Base Sector


Government Facilities Sector


Transportation Systems Sector


Commercial Facilities Sector


Emergency Services Sector


Healthcare and Public Health Sector


Water and Wastewater Systems Sector


Communications Sector


Energy Sector

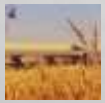

Information Technology Sector


Critical Manufacturing Sector


Financial Services Sector


Nuclear Reactors, Materials, and Waste Sector


Dams Sector


Food and Agriculture Sector

# NIST FRAMEWORK UPDATE

**FEB 12, 2013 EXECUTIVE ORDER**

- EXECUTIVE ORDER 13636 – *IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY*

**FEB 12, 2014 FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBER SECURITY, V1.0**

**COMPENDIUM OF INFORMATIVE REFERENCES**

- REVIEW OF OVER 320 NATIONAL & INTERNATIONAL STANDARDS, GUIDELINES, DIRECTIVES, BEST PRACTICES, MODELS, SPECIFICATIONS, POLICIES AND REGULATIONS, INCLUDING INPUT FROM:

| | | |
|---|---|---|
| ANSI | IEC | OLF |
| ISA | NEI | OPC |
| NERC | NIST | SANS |
| API | NFPA | TIA |
| ISO | OIG | |

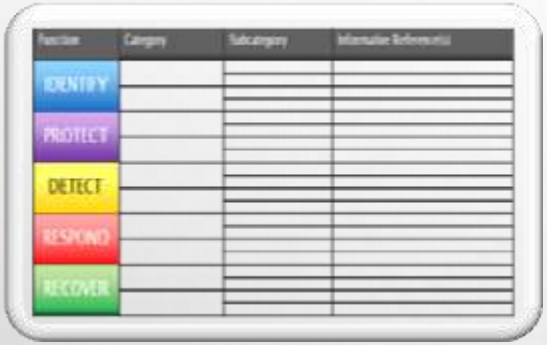
# NIST FRAMEWORK CONCEPTS

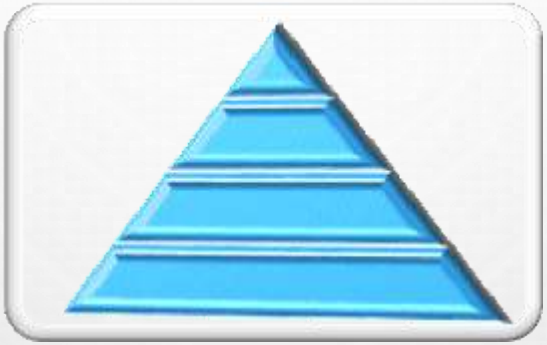
- THE FRAMEWORK **COMPLEMENTS**, AND **DOES NOT REPLACE**, AN ORGANIZATION'S EXISTING BUSINESS OR CYBERSECURITY RISK MANAGEMENT PROCESS AND CYBERSECURITY PROGRAM. RATHER, THE ORGANIZATION CAN USE ITS CURRENT PROCESSES AND LEVERAGE THE FRAMEWORK TO IDENTIFY OPPORTUNITIES TO IMPROVE AN ORGANIZATION'S CYBERSECURITY RISK MANAGEMENT. ALTERNATIVELY, AN ORGANIZATION WITHOUT AN EXISTING CYBERSECURITY PROGRAM CAN USE THE FRAMEWORK AS A REFERENCE WHEN ESTABLISHING ONE.

## KEY CONCEPTS

- FRAMEWORK CORE
- FRAMEWORK IMPLEMENTATION TIERS
- FRAMEWORK PROFILE

# NIST FRAMEWORK CONCEPTS




## CORE

FUNCTIONS

CATEGORIES

SUBCATEGORIES

INFORMATIVE REFERENCE

## TIER

0 - PARTIAL

1- RISK INFORMED

2 - REPEATABLE

3 - ADAPTIVE

## PROFILE

ESTABLISH A ROADMAP

# FRAMEWORK CORE

| Function | Category | Subcategory | Informative Reference(s) |
|---|---|---|---|
| IDENTIFY | | | |
| PROTECT | | | |
| DETECT | | | |
| RESPOND | | | |
| RECOVER | | | |

# NIST FRAMEWORK
## FUNCTIONS

**IDENTIFY**

- DEVELOP THE ORGANIZATIONAL UNDERSTANDING TO MANAGE CYBERSECURITY RISK TO SYSTEMS, ASSETS, DATA, AND CAPABILITIES.
- THE ACTIVITIES IN THE IDENTIFY FUNCTION ARE FOUNDATIONAL FOR EFFECTIVE USE OF THE FRAMEWORK. UNDERSTANDING THE BUSINESS CONTEXT, THE RESOURCES THAT SUPPORT CRITICAL FUNCTIONS, AND THE RELATED CYBERSECURITY RISKS ENABLES AN ORGANIZATION TO FOCUS AND PRIORITIZE ITS EFFORTS, CONSISTENT WITH ITS RISK MANAGEMENT STRATEGY AND BUSINESS NEEDS. EXAMPLES OF OUTCOME CATEGORIES WITHIN THIS FUNCTION INCLUDE: ASSET MANAGEMENT; BUSINESS ENVIRONMENT; GOVERNANCE; RISK ASSESSMENT; AND RISK MANAGEMENT STRATEGY.

# NIST FRAMEWORK
## CYBERSECURITY CONTROLS

**IDENTIFY**

| *PLANT REFERENCE* | CYBER CONTROL |
| --- | --- |
| *POLICIES* | POLICIES |
| *ROLES & RESPONSIBILITIES* | ROLES & RESPONSIBILITIES |
| *RISK ASSESSMENT* | VULNERABILITY ASSESSMENT |
| *EQUIPMENT LIST* | ASSET / APPLICATION LIST |
| *AREA / PROCESS CLASSIFICATION* | ASSET / APPLICATION CLASSIFICATION |
| *P&ID'S* | NETWORK DIAGRAMS |

# NIST FRAMEWORK
## FUNCTIONS

**PROTECT**

- DEVELOP AND IMPLEMENT THE APPROPRIATE SAFEGUARDS TO ENSURE DELIVERY OF CRITICAL INFRASTRUCTURE SERVICES.
- THE PROTECT FUNCTION SUPPORTS THE ABILITY TO LIMIT OR CONTAIN THE IMPACT OF A POTENTIAL CYBERSECURITY EVENT. EXAMPLES OF OUTCOME CATEGORIES WITHIN THIS FUNCTION INCLUDE: ACCESS CONTROL; AWARENESS AND TRAINING; DATA SECURITY; INFORMATION PROTECTION PROCESSES AND PROCEDURES; MAINTENANCE; AND PROTECTIVE TECHNOLOGY.

# NIST FRAMEWORK
## CYBERSECURITY CONTROLS

**PROTECT**

| *PLANT REFERENCE* | CYBER CONTROL |
|---|---|
| *TRAINING* | TRAINING |
| *BACKGROUND CHECKS* | ANTI-VIRUS & PATCHING |
| *GUARDS* | FIREWALLS |
| *CARD KEYS / BADGES* | CARD KEYS / BADGES |
| *ESCORTED ACCESS* | ESCORTED ACCESS |
| *KEYED LOCKS / LOTO* | LOGICAL ACCESS CONTROL |
| *LEAST PRIVILEGE ACCESS* | LEAST PRIVILEGE ACCESS |
| *PROCEDURES* | PROCEDURES |
| *JOB SAFETY ASSESSMENT* | CONFIGURATION CHANGE MANAGEMENT |

# NIST FRAMEWORK
## FUNCTIONS

**DETECT**

- DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO IDENTIFY THE OCCURRENCE OF A CYBERSECURITY EVENT.
- THE DETECT FUNCTION ENABLES TIMELY DISCOVERY OF CYBERSECURITY EVENTS. EXAMPLES OF OUTCOME CATEGORIES WITHIN THIS FUNCTION INCLUDE: ANOMALIES AND EVENTS; SECURITY CONTINUOUS MONITORING; AND DETECTION PROCESSES.

# NIST FRAMEWORK
## CYBERSECURITY CONTROLS

**DETECT**

*PLANT REFERENCE*

- *LOGS / OPERATOR ROUNDS*
- *CAMERA / MOTION DETECT*
- *ANALYZERS*
- *ALARMS / ALERTS*
- *UNAUTHORIZED PERSONNEL INTERVENTION*

→ CYBER CONTROL

- LOGS, SECURITY INFORMATION & EVENT MONITOR (SIEM)
- INTRUSION DETECTION
- NETWORK PERFORMANCE MONITORING
- ALARMS / ALERTS
- ROGUE DEVICE DETECTION

# NIST FRAMEWORK
## FUNCTIONS

**RESPOND**

- DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO TAKE ACTION REGARDING A DETECTED CYBERSECURITY EVENT.
- THE RESPOND FUNCTION SUPPORTS THE ABILITY TO CONTAIN THE IMPACT OF A POTENTIAL CYBERSECURITY EVENT. EXAMPLES OF OUTCOME CATEGORIES WITHIN THIS FUNCTION INCLUDE: RESPONSE PLANNING; COMMUNICATIONS; ANALYSIS; MITIGATION; AND IMPROVEMENTS.

# NIST FRAMEWORK
## CYBERSECURITY CONTROLS

**RESPOND**

| *PLANT REFERENCE* | CYBER CONTROL |
| --- | --- |
| • *EMERGENCY RESPONSE PLANNING* | • EMERGENCY RESPONSE PLANNING |
| • *EXECUTE EMERGENCY RESPONSE PLAN* | • EXECUTE EMERGENCY RESPONSE PLAN |
| • *NOTIFY AUTHORITIES* | • NOTIFY AUTHORITIES |
| • *ISOLATE & PRESERVE* | • ISOLATE & PRESERVE |
| • *INITIATE RECOVERY* | • INITIATE RECOVERY |
| • *UPDATE RESPONSE PLAN* | • UPDATE RESPONSE PLAN |

# NIST FRAMEWORK
## FUNCTIONS

**RECOVER**

- DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO MAINTAIN PLANS FOR RESILIENCE AND TO RESTORE ANY CAPABILITIES OR SERVICES THAT WERE IMPAIRED DUE TO A CYBERSECURITY EVENT.
- THE RECOVER FUNCTION SUPPORTS TIMELY RECOVERY TO NORMAL OPERATIONS TO REDUCE THE IMPACT FROM A CYBERSECURITY EVENT. EXAMPLES OF OUTCOME CATEGORIES WITHIN THIS FUNCTION INCLUDE: RECOVERY PLANNING; IMPROVEMENTS; AND COMMUNICATIONS.

# NIST FRAMEWORK
## CYBERSECURITY CONTROLS

**RECOVER**

| *PLANT REFERENCE* | CYBER CONTROL |
| --- | --- |
| *BYPASS* | ALTERNATE CONTROLS |
| *IMPLEMENT SPARE* | IMPLEMENT SPARE |
| *REPAIR/REBUILD/REPLACE* | REPAIR/REBUILD/REPLACE |
| *RESET* | RESET |

# GET HELP

- REGULATORY BODY
- RESEARCHERS
- VENDORS
- CONSULTANTS

American Water Works Association (AWWA)
http://www.awwa.org/resources-tools/water-utility-management/cybersecurity-guidance.aspx

National Institute of Standards and Technology (NIST)
Computer Security Division
www.nist.gov/itl/csd/

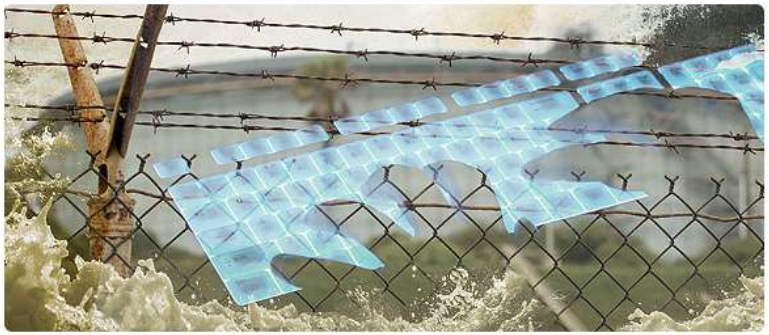
United States Computer Emergency Readiness Team (US-CERT)
www.us-cert.gov

Critical Infrastructure & Security Practice (CISP)
iom.invensys.com/cybersecurity
gary.kneeland@schneider-electric.com

AFFORDABILITY ASSESSMENT
BENCHMARKING
COLLABORATION
CYBERSECURITY GUIDANCE
EFFECTIVE UTILITY MANAGEMENT
HYPOCHLORITE ASSESSMENT MODEL
PARTNERSHIP FOR SAFE WATER
STATE OF THE WATER INDUSTRY
WATER & WASTEWATER RATES



## Cybersecurity Guidance & Tool



Cybersecurity is the top threat facing business and critical infrastructure in the United States, according to reports and testimony from the National Intelligence Agency, the Federal Bureau of Investigation and the Department of Homeland Security.

Based on recommendations in the 2008 Roadmap to Secure Industrial Control Systems in the Water Sector, AWWA's Water Utility Council took action to develop a cybersecurity resource designed to provide actionable information for utility owner/operators based on their use of process control systems. That is the purpose and objective of the Process Control System Security Guidance for the Water Sector (PDF) and the supporting Use-Case Tool.

These AWWA resources complement the national-level actions that have resulted from Executive Order 13636 - Improving Critical Infrastructure Cybersecurity, signed by President Obama on Feb. 12, 2013. EO 13636 directs the National Institute of Standards and Technology to work with stakeholders to develop a voluntary framework for reducing cyber risks, recognizing that national and economic security depends on the reliable functioning of critical infrastructure.

The AWWA Cybersecurity Guidance & Tool represent a voluntary, sector-specific approach that supports 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.

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

Access additional AWWA resources on **Utility Security** and on **Emergency Preparedness**

## Cybersecurity Tool

A use case is an elemental pattern of behavior as described by the user of a system. The use cases presented in the AWWA Cybersecurity Guidance Tool are intended to reflect the manner in which a user's Process Control System is configured and/or the manner in which the organization utilizes the Process Control System. The operational characteristics associated with each use case represent different types and degrees of cybersecurity risk. The guidance tool determines the appropriate cybersecurity controls and priorities based on the use cases selected by the user.

Prior to using the Guidance Tool, the user should review specific information pertaining to the organization's Process Control Systems, including device inventory, network architecture, software functionality, physical facility and plant process architecture. With some utilities, this knowledge is spread among several individuals and/or departments; certain aspects of this detailed knowledge may be held by vendors or external service providers. Conducting a planning meeting with the appropriate resources and stakeholders prior to using the Guidance Tool should be considered.

There is a wide variety of different products and system configurations used for water sector Process Control Systems. As such, some of the use cases provided may not match a user's specific situation exactly. In that case, the user should select the use cases which most closely match the utility's systems and procedures.

---

**Use Cases:** (check all that apply)

CLEAR ALL

### Architecture

- ☐ **AR1: Dedicated network.** All network and communications infrastructure is dedicated exclusively to SCADA. No connection to enterprise networks.
- ☐ **AR2: Shared WAN.** Wide-area network communications infrastructure is shared (controls: physical (media) separation, VPN, VLAN, firewall).
- ☐ **AR3: Shared LAN.** Local-area network communications (within facility) is shared (controls: VLAN, firewall).

### Network Management

- ☐ **NM1: Local network management.** Access to configure network infrastructure located in immediate vicinity of user (serial or network).
- ☐ **NM2: Plant network management.** Access to configure network infrastructure located on same facility from centralized location.
- ☐ **NM3: Remote network management.** Access to configure network infrastructure located in another physical facility.

### Program Access

- ☐ **PA1: Outbound messaging.** Automated, non-interactive sending of SMTP, SMS or other outbound alarms and messaging from system.

- [ ] **PA2: Outbound file transfer.** Interactive sending of files from system to other locations.
- [ ] **PA3: Inbound file transfer.** Interactive receiving of files from other locations to system.
- [ ] **PA4: Software updates.** Automated, non-interactive retrieval of licensing, OS updates, anti-virus signatures and other system data from other locations to system.
- [ ] **PA5: Data exchange.** Automated, non-interactive exchange of data (e.g. database-to-database exchange, ntp or other external data) with systems located externally. (Implies full-time connection.)
- [ ] **PA6: Network monitoring.** Automated, non-interactive exchange of network management data (e.g. syslog, SNMP traps, SNMP polling) with system(s) located external to system. (Implies full-time connection.)

### PLC Programming and Maintenance

- [ ] **PLC1: Local PLC programming and maintenance.** Access to PLC programming and maintenance is local to device (serial or network).
- [ ] **PLC2: Plant PLC programming and maintenance.** Access to PLC programming and maintenance from a centralized on-site location.
- [ ] **PLC3: Remote PLC programming and maintenance.** Access to PLC programming and maintenance from an off-site location.

### User Access

- [ ] **UA1: Control room system access with control.** Access to system with full read-write capability from "control room" (on-plant, physically secured) location.
- [ ] **UA2: Plant system access with control.** Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor).
- [ ] **UA3: Remote system access with control.** Access from location outside "control room" environment and located outside the physical perimeter of the facility.
- [ ] **UA4: Remote system access with view-only.** Access to system with limited read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility.
- [ ] **UA5: Remote system access with web view.** Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility.

By clicking "Generate Report" you accept AWWA's **terms and conditions**.

GENERATE REPORT

# THANK YOU