

**Colorado Federal Executive Board
Mile High DICE
Cybersecurity Seminar and
Tabletop Exercise**

**Cybersecurity
Resource Reference
Aid**



November 10, 2016

CFEB Website: colorado.feb.gov

**National Institute of Standards and Technology
(NIST) Cybersecurity Framework**

The framework is a collaborative effort between government and private sector that makes use of a common language to address and manage cybersecurity risks.

Purpose: Improve cybersecurity of U.S. critical infrastructure by enabling organizations to apply the principles and best practices of risk management.

The framework provides a common taxonomy and mechanism for organizations to:

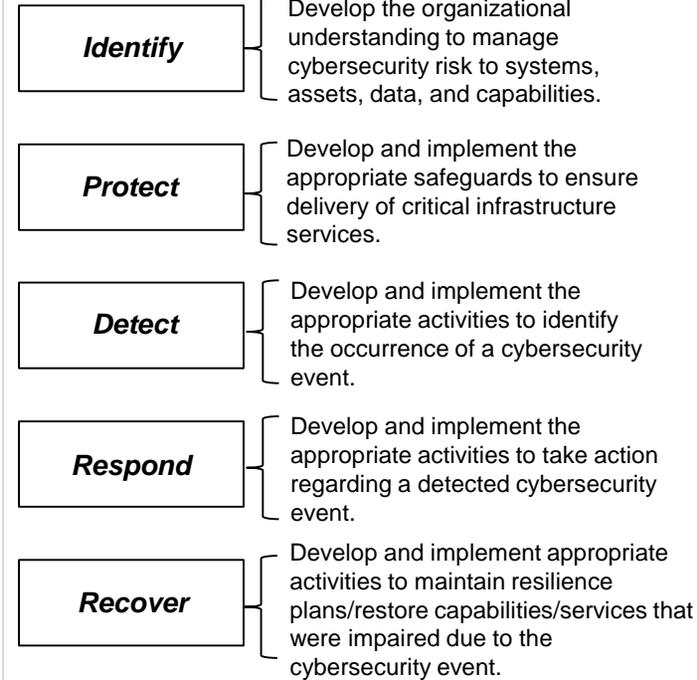
- 1) Describe their current cybersecurity posture
- 2) Describe their target state for cybersecurity
- 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- 4) Assess progress toward the target state
- 5) Communicate among internal and external stakeholders about cybersecurity risk

NIST Cybersecurity Framework:

<https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

NIST Cybersecurity Functions

The functions provide a comprehensive perspective for building Cybersecurity related plans, policies, and procedures.



Risk Management and Assessment

- **Cybersecurity Capability Maturity Model (C2M2):** <https://niccs.us-cert.gov/research/cybersecurity-capability-maturity-model>
- **Cybersecurity Evaluation Tool (CSET):** <https://ics-cert.us-cert.gov/Assessments>
- **Cyber Resilience Review:** <https://www.us-cert.gov/ccubedvp/assessments>
- **NIST SP 800-39, Managing Information Security Risk:** <http://dx.doi.org/10.6028/NIST.SP.800-39>
- **FFIEC Cybersecurity Assessment Tool:** <https://www.ffiec.gov/cyberassessmenttool.htm>
- **Electricity Subsector Cybersecurity Risk Management Process:** <http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf>
- **Cybersecurity Questions for CEOs:** <https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf>

Risk Management and Assessment

- **Guide for Applying the Risk Management Framework to Federal Information Systems:** <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf>
- **Risk Management Framework (RMF) for DoD Information Technology (IT):** http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
- **OCIE's 2015 Cybersecurity Examination Initiative:** <https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf>
- **Improving Third Party Risk Management with Cyber Threat Intelligence:** <http://www.isaca.org/chapters11/Western-New-York/Events/Documents/2015-April/CT02-3RD-Party-Cybersecurity-NMenz.pdf>
- **Information Security Risk Assessment Checklist:** <http://www.cio.ca.gov/OIS/government/risk/toolkit.asp>

Cybersecurity Planning

- **NIST SP 800-53 rev 4, Assessing Security/Privacy Controls in Federal Information Systems and Organizations:** <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>
- **NIST Cyber Supply Chain Best Practices:** <https://www.nist.gov/sites/default/files/documents/it/csd/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.Pdf>
- **Cybersecurity Workforce Development Toolkit:** <https://niccs.us-cert.gov/research/documents>
- **Cybersecurity Workforce Planning Diagnostic:** <https://niccs.us-cert.gov/careers/cybersecurity-workforce-planning-diagnostic>
- **Tools and Resources to Build Your Cybersecurity Workforce:** [https://www.fbcinc.com/e/nice/ncec/presentations/2015/Scribner_\(Tools\).pdf](https://www.fbcinc.com/e/nice/ncec/presentations/2015/Scribner_(Tools).pdf)
- **FCC Cybersecurity Planning Guide:** https://www.dhs.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide_1.pdf

Cybersecurity Planning

- **A Non-Technical Cybersecurity Guide for Local Leaders:**
<https://www.osc.state.ny.us/localgov/lgli/pdf/cybersecurityguide.pdf>
- **Internet Security Essentials for Business 2.0:**
<https://www.uschamber.com/sites/default/files/legacy/issuess/technology/files/ISEB-2.0-CyberSecurityGuide.pdf>
- **Best Practices for Building a Cybersecurity Workforce:**
http://csrc.nist.gov/nice/documents/best_practices_for_planning_a_cybersecurity_workforce_05312012_v4_1_draft_nice_branded.pdf
- **Lessons Learned from Cybersecurity Assessments of SCADA and Energy Management Systems:**
http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/1-NTB_Control_Systems_Security_Standards_Accomplishments_and_Impacts.pdf
- **AWA Process Control System Security Guidance for the Water Sector:** <http://www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf>

Cybersecurity Planning

- **TSA Pipeline Security Guidelines:**
<https://www.tsa.gov/sites/default/files/tsapipelinecurityguidelines-2011.pdf>
- **Cybersecurity for Small Businesses:**
<https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses>
- **IT Disaster Recovery Plan:**
<https://www.ready.gov/business/implementation/IT>
- **FINRA Report on Cybersecurity Practices:**
http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf
- **Hospital Cybersecurity Planning Quick Reference Tool:**
http://www.calhospital.org/sites/main/files/file-attachments/hospital_cybersecurity_planning_quick_reference_tool.pdf
- **Protecting the Healthcare Digital Infrastructure Cybersecurity Checklist:**
<http://www.phe.gov/Preparedness/planning/cip/Documents/cybersecurity-checklist.pdf>

Federal Cybersecurity Organizations And Programs

- **Office of Cybersecurity and Communications (CS&C):**
<https://www.dhs.gov/office-cybersecurity-and-communications>
- **National Cybersecurity and Communications Integration Center (NCCIC):** <https://www.dhs.gov/national-cybersecurity-and-communications-integration-center>
- **U.S. Computer Emergency Readiness Team (US-CERT):**
<https://www.us-cert.gov/>
- **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT):** <https://ics-cert.us-cert.gov/>
- **Critical Infrastructure Cyber Community Voluntary Program (C3VP):** <https://www.us-cert.gov/ccubedvp>
- **National Cyber Exercise and Planning Program (NCEPP):** Email at CEP@hq.dhs.gov

Presidential Policy Directive 41—U.S. Cyber Incident Coordination: <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

National Security Agency's Top 10 Cybersecurity Controls

- GOALS {
- Device Integrity
 - Damage Containment
 - Defense of Accounts
 - Secure and Available Transport of Data

- Application Whitelisting
- Control Administrative Privileges
- Limit Workstation-to-Workstation Communication
- Use Anti-Virus File Reputation Services
- Enable Anti-Exploitation Features
- Implement Host Intrusion Prevention System Rules
- Set a Secure Baseline Configuration
- Use Web Domain Name System Reputation
- Take Advantage of Software Improvements
- Segregate Networks and Functions

NSA Top 10 Cybersecurity Controls:

https://www.sans.org/security-resources/IAD_top_10_info_assurance_mitigations.pdf

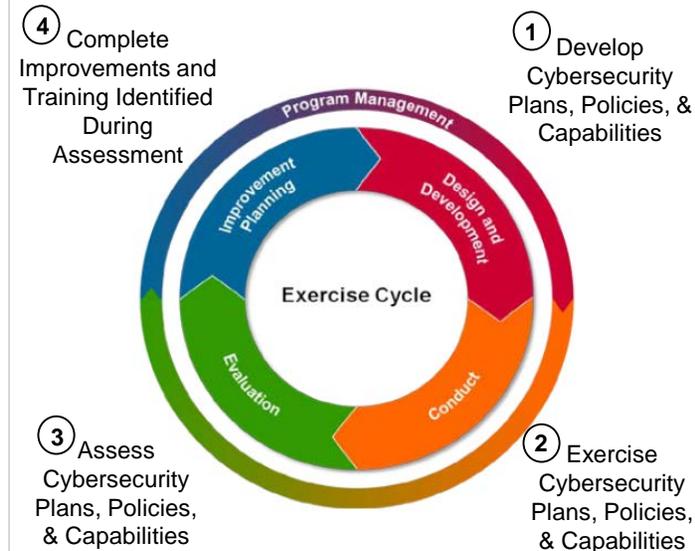
Critical Infrastructure Information Sharing

- **Colorado Information Analysis Center:** report.ciac.co.gov
- **Multi-State-Information Sharing and Analysis Center (ISAC):** www.ms-isac.org
- **Information Technology-ISAC:** www.it-isac.org
- **Electricity-ISAC:** www.esisac.com
- **Water-ISAC:** www.waterisac.org
- **Oil and Natural Gas-ISAC:** www.ongisac.org
- **Financial Services-ISAC:** www.fsisac.com
- **National Health-ISAC:** www.nhisac.org
- **Supply Chain-ISAC:** www.sc-isac.org
- **Aviation-ISAC:** www.a-isac.com
- **Emergency Management/Response-ISAC:**
https://www.usfa.fema.gov/operations/ops_cip.html

Homeland Security Critical Infrastructure Sector Specific Plans:

<https://www.dhs.gov/critical-infrastructure-sectors>

Integrating Training and Exercises into Cybersecurity Efforts



Homeland Security Exercise and Evaluation Program Document Location:

<https://www.fema.gov/media-library/assets/documents/32326>