

Framework for Improving Critical Infrastructure Cybersecurity

September 2016

cyberframework@nist.gov

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Why Consider Cybersecurity Framework

Relevance of Framework to HPC Security

- It Defines a Complete Spectrum of Cybersecurity Considerations
- Connects Technologists with the Leadership Teams that Support Them
- It is Widely Used and that Use is Increasing

Defines Cybersecurity Considerations

Relevance of Framework to HPC Security

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
What safeguards are available?	Protect	Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

Connects Technologists with Leadership

Relevance of Framework to HPC Security

<p>PROTECT (PR)</p>	<p>Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.</p>	<p>PR.AC-1: Identities and credentials are managed for authorized devices and users</p>	<ul style="list-style-type: none"> • CCS CSC 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-2, IA Family
		<p>PR.AC-2: Physical access to assets is managed and protected</p>	<ul style="list-style-type: none"> • COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 • ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		<p>PR.AC-3: Remote access is managed</p>	<ul style="list-style-type: none"> • COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6 • ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1

Widely Used

Relevance of Framework to HPC Security

- Is broadly used in private sector - Gartner projects 30% use currently in the U.S., trending to 50% by 2020
- Is acknowledged as voluntary for Federal organizations - updated OMB Circular A-130
- Known to be used by 32% of States in the U.S. and is the basis of the Multi-State ISAC in their National Cybersecurity Assessment
- Is gaining momentum internationally - NIST has dialogued with 29 governments and ANSI→ISO/ISE

Learning More

Where to Learn More and Stay Current

*Framework for Improving Critical Infrastructure
Cybersecurity* and related news, information:

www.nist.gov/cyberframework

Additional cybersecurity resources:

<http://csrc.nist.gov/>

Questions, comments, ideas:

cyberframework@nist.gov

