CISA Cross-Sector Cybersecurity Performance Goals

A baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value.
A benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity.
A combination of recommended practices for IT and OT owners, including a prioritized set of security practices.

Unique from other control frameworks as they consider not only the practices that address risk to individual entities, but also the aggregate risk to the nation.

Website: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Checklist: https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist

Report: https://www.cisa.gov/resources-tools/resources/cpg-report

Spreadsheet: https://www.cisa.gov/resources-tools/resources/complete-cpgs-matrixspreadsheet

Security benchmark	Cost	Complexity	Impact
Detection of unsuccessful (automated) login attempts	$	Low	High
Changing default passwords	$	Medium	High
Mutlifactor authentication (MFA)	$$	Medium	High
Minimum password strength	$	Low	High
Separating user and privileged accounts	$	Low	High
Unique credentials	$$	Medium	Medium
Revoking credentials for departing employees	$	Low	Medium
Hardware and software approval process	$$	Medium	High
Disable macros by default	$	Low	Medium
Asset inventory	$$	Medium	High
Prohibit connection of unauthorized devices	$$$	High	High
Document device configurations	$$	Medium	High
Log collection	$$	Medium	High
Secure log storage	$$$	Low	High
Asset inventory	$$	Medium	High
Secure sensitive data	$$	Medium	High
Organizational cybersecurity leadership	$	Low	High
OT cybersecurity leadership	$	Low	High
Basic cybersecurity training	$	Low	High
OT cybersecurity training	$	Low	High
Improving IT and OT cybersecurity relationships	$	Low	Medium
Mitigating known vulnerabilities	$	Medium	High
Vulnerability disclosure/reporting	$$$	High	Low
Deploy security.txt files	$	Low	High
No exploitable services on the internet	$	Low	High
Limit OT connections to public internet	$$$	Medium	Medium
Third-party validation of cybersecurity control effectiveness	$$$	High	High
Vendor/supplier cybersecurity requirements	$	Low	High
Supply chain incident reporting	$	Low	High
Supply chain vulnerability disclosure	$	Low	High
Incident reporting	$	Low	High
Incident response plans	$	Low	High
System back ups	$$	Medium	High
Document network topology	$$	Medium	Medium
Network segmentation	$$$	High	High
Detecting relevant threats and TTPs	$$$	High	Medium
Email security	$	Low	Medium