3RD ANNUAL NATIONAL

CYBERSECURITY SUMMIT

Recommended Cybersecurity Practices for Industrial Control Systems

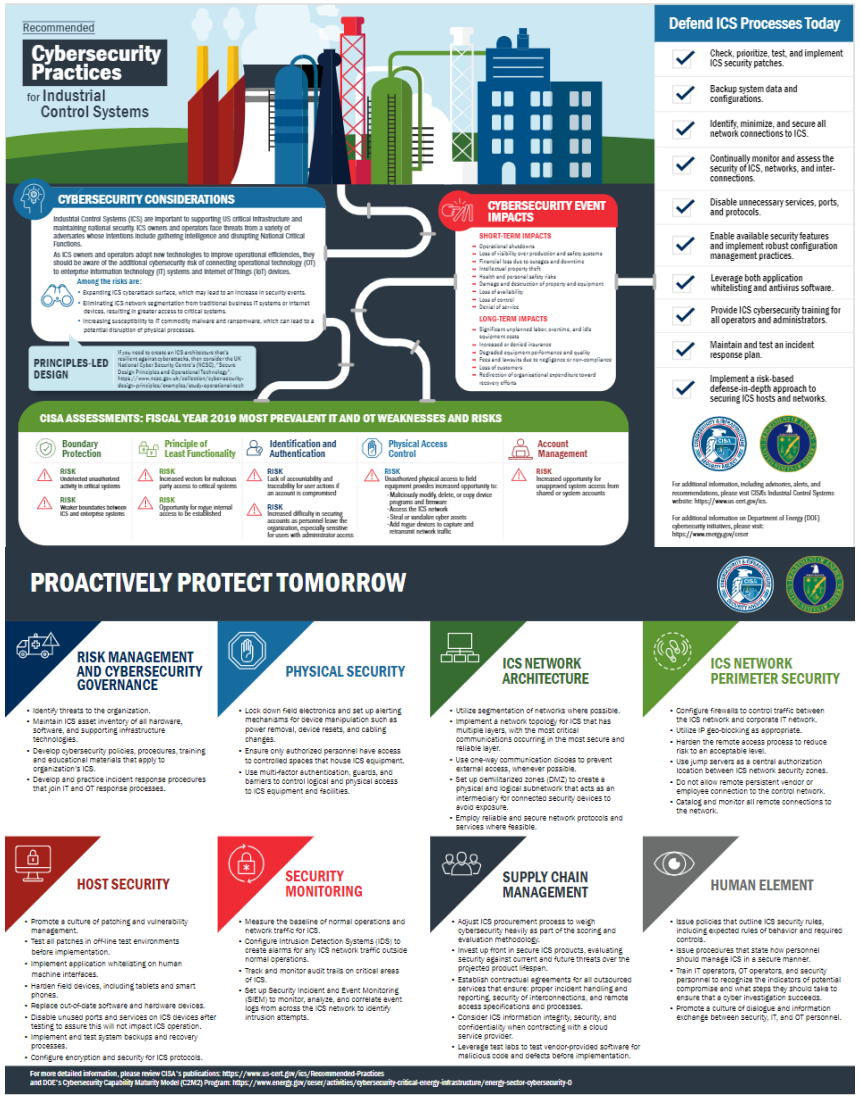
3RD ANNUAL NATIONAL CYBERSECURITY SUMMIT

Infographic Background

Cybersecurity and Infrastructure Security Agency (CISA) and Department of Energy (DOE) hope to emphasize the importance of securing Industrial Control Systems (ICS).

Development of this product was collaborative with contributions from CISA, DOE, the United Kingdom's National Cyber Security Centre (NCSC), and members of CISA's ICS Joint Working Group.

Leveraged leading research and approaches for ICS cybersecurity.



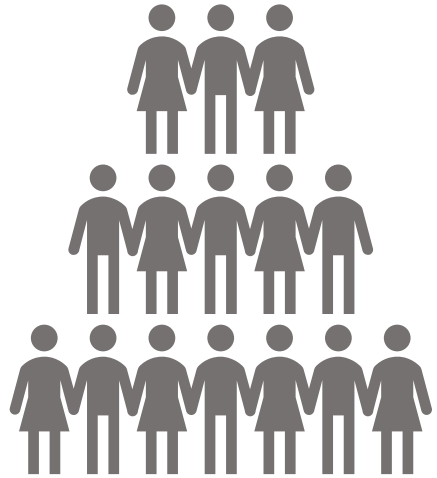
3RD ANNUAL NATIONAL CYBERSECURITY SUMMIT

ICS Cyber Infographic Purpose

Call attention to the importance of ICS to critical infrastructure and start a conversation about proactive measures to defend ICS from cyber attacks

Encourage communication between owners and operators, including the following audience:

- Organization leaders and decision makers (C-suite, board members)
- ICS professionals (control engineers, technicians, and operators)
- IT professionals (cybersecurity, engineering, and architecture)



Highlight key aspects of ICS cybersecurity:

1. Current state of ICS cybersecurity
2. ICS risks and weaknesses identified via assessments
3. Impacts of cyber attacks on ICS
4. Immediate actions to defend ICS from cyber attack
5. Longer term strategic programs to defend ICS

ICS Cybersecurity Considerations

ICS owners and operators face threats from adversaries who intend to disrupt critical infrastructure. Highlighted risks include:

- Expanding ICS cyberattack surface, which may lead to an increase in security events.
- Eliminating ICS network segmentation from traditional business IT systems or internet devices, resulting in greater access to critical systems.
- Increasing susceptibility to IT commodity malware and ransomware, which can lead to a potential disruption of physical processes.

Recent real world ICS cyber attack themes:

- Phishing attacks to gain initial access
- Malware built to attack and leverage ICS protocols
- Initial compromise of IT networks, followed by exploit to spread to operational networks

CISA Assessments

CISA assessment of critical infrastructure entities can identify risks and weaknesses in ICS. CISA Assessments:

- Are conducted in partnership with ICS stakeholders
- Assess aspects of critical infrastructure (cybersecurity controls, control system architectures, adherence to best practices, etc.)
- Provide recommendations to mitigate and manage risk
- Improve situational awareness
- Provide insight, data, and identification of control system threats and vulnerabilities

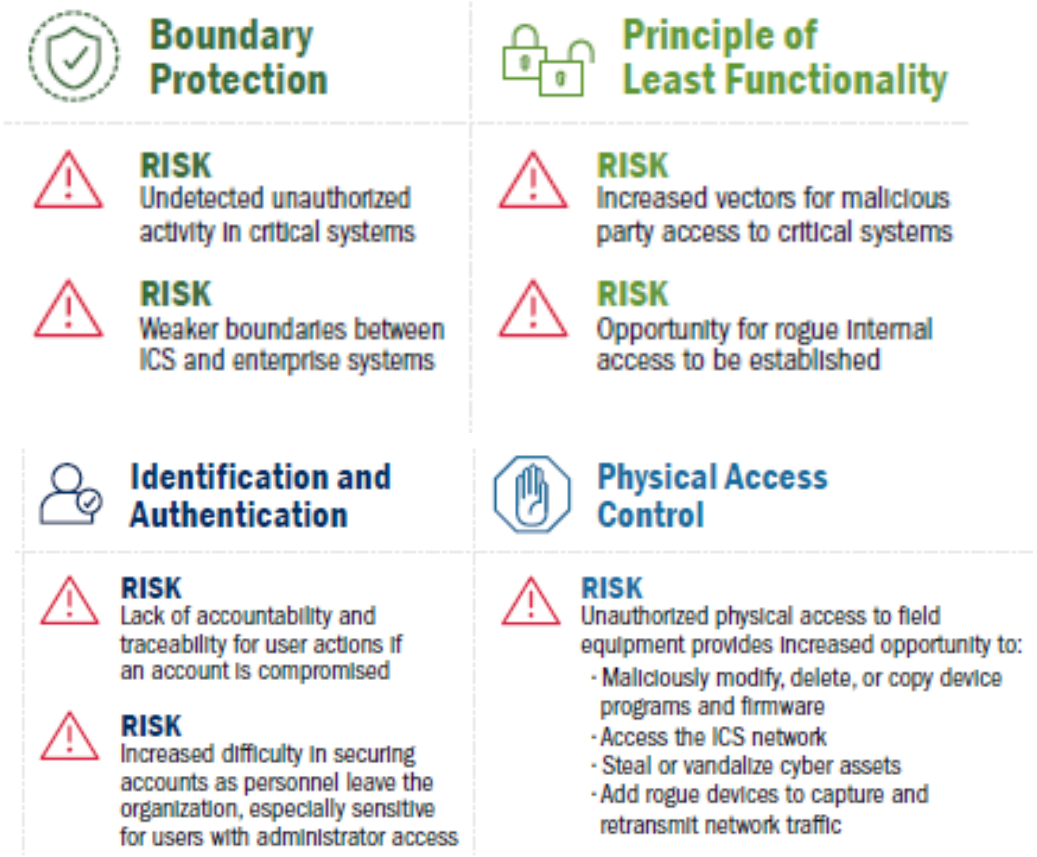
Assessment information provides stakeholders with the understanding and context necessary to build effective cybersecurity processes.

CISA Assessments

Recommendations in the infographic are backed by assessment data showing the most pertinent ICS cybersecurity risks today.

Critical infrastructure assessments included:

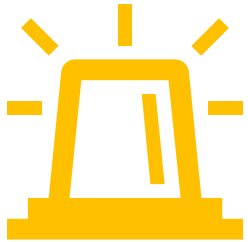
- Phishing Campaign Assessments (PCA)
- Risk Vulnerability Assessments (RVA)
- Validated Architecture Design Reviews (VADR)
- Cyber Hygiene (CyHy)



Impacts of ICS Cyber Attacks

Short-term, immediate impacts of successful ICS cyber attacks include:

- Loss of visibility over production and safety systems
- Financial loss due to outages and downtime
- Health and personal safety risks
- Damage and destruction of property and equipment



Long-term impacts of successful ICS cyber attacks include:

- Significant unplanned labor, overtime, and idle equipment costs
- Increased or denied insurance
- Fees and lawsuits due to negligence or non-compliance
- Loss of customers

Defend ICS Processes Today

Recommended cybersecurity practices to implement immediately:

- Check, prioritize, test, and implement ICS security patches.
- Backup system data and configurations.
- Identify, minimize, and secure all network connections to ICS.
- Continually monitor and assess the security of ICS, networks, and inter-connections.
- Disable unnecessary services, ports, and protocols.
- Enable available security features and implement robust configuration management practices.
- Leverage both application whitelisting and antivirus software.
- Provide ICS cybersecurity training for all operators and administrators.
- Maintain and test an incident response plan.
- Implement a risk-based defense-in-depth approach to securing ICS hosts and networks.

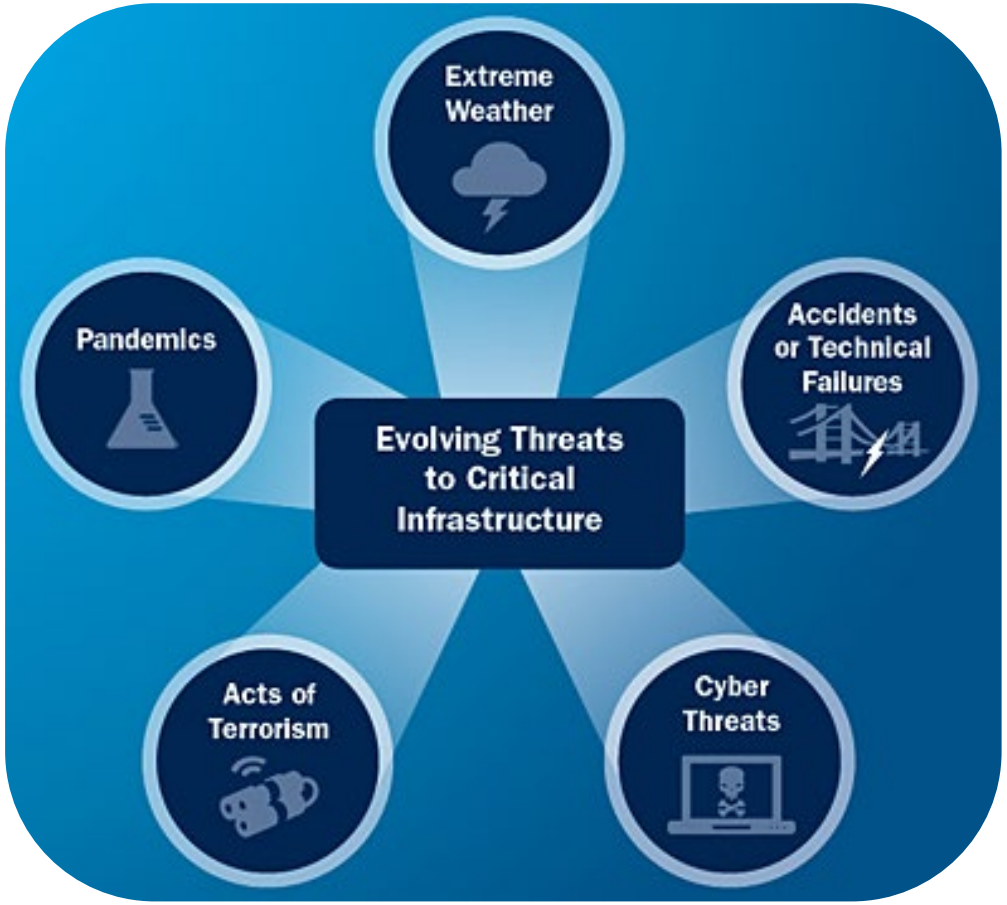
Defend ICS Processes Today

Long-term defensive strategies for ICS cybersecurity are grouped into the following categories:

Critical Infrastructure in the US

DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Mission

CESER leads the Department's efforts to secure U.S. energy infrastructure against all threats and hazards, reduce the risks of and impacts from disruptive events, and facilitates restoration activities.



Cybersecurity for the Operational Technology Environment (CyOTE)

Goal: The CyOTE program aims to enhance threat detection in critical operational technology (OT) systems by adding insight from US intelligence.

Objectives:

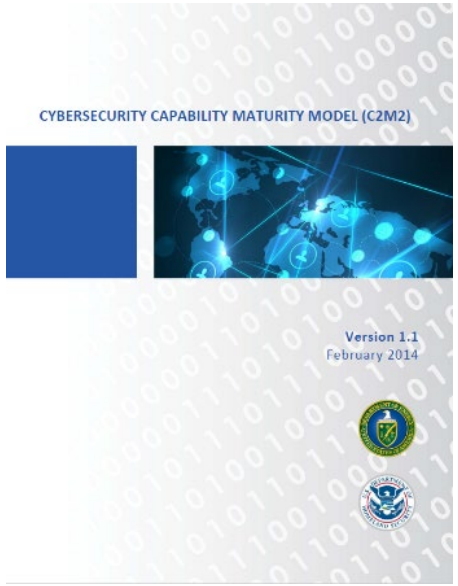
- Map the OT cyber "kill chain" for potential attack pathways to OT systems
- Identify points within OT systems to monitor and share data;
- Install monitoring at those points; identify trusted mechanisms to share key data;
- Analyze operational utility data from OT environments;
- Provide sector partners with expert analysis and threat information to bring a classified context; and
- Evaluate the feasibility of a repeatable, industry-wide approach for OT threat data analysis.

Cyber Testing for Resilience of the Industrial Control Systems (CyTRICS)

- **Goal:** The CyTRICS™ program is intended to strengthen energy sector supply chain cybersecurity and resilience.
- **Objectives:**
  - Prioritize risks related to the supply chain for ICS, OT, and other critical components used in the energy sector
  - Understand and mitigate vulnerabilities in critical energy sector equipment
  - Develop a energy sector focused cyber vulnerability disclosure (CVD) program for operational technology in the energy sector
  - Inform design and manufacturing decisions for critical components
  - Create actionable intelligence through the linkage of threat information with supply chain information

Cybersecurity Capability Maturity Model (C2M2)

Goal: A voluntary evaluation process utilizing industry-accepted cybersecurity practices that can be used to measure the maturity of an organization's cybersecurity capabilities.



Objectives:

- Provide a measure of the sophistication and sustainment of a cyber security program.
- Develop a logical understanding and measurement of policies, processes, and procedures involved in an organization's cyber security posture.
- Provide **maturity** indicator levels (MILs) to discuss an organization's operational capabilities and management of cybersecurity risk.

Next Steps

1. Share the infographic with interested partners.
2. Start a larger discussion about the evolving vulnerabilities, threats, and impacts facing ICS and emphasize that proactive countermeasures can be implemented today.
3. Connect with CISA and DOE to contribute to the discussion about ICS cybersecurity.
4. Let your stakeholders know that they can reach out to CISA and DOE for advice and support regarding protecting ICS.

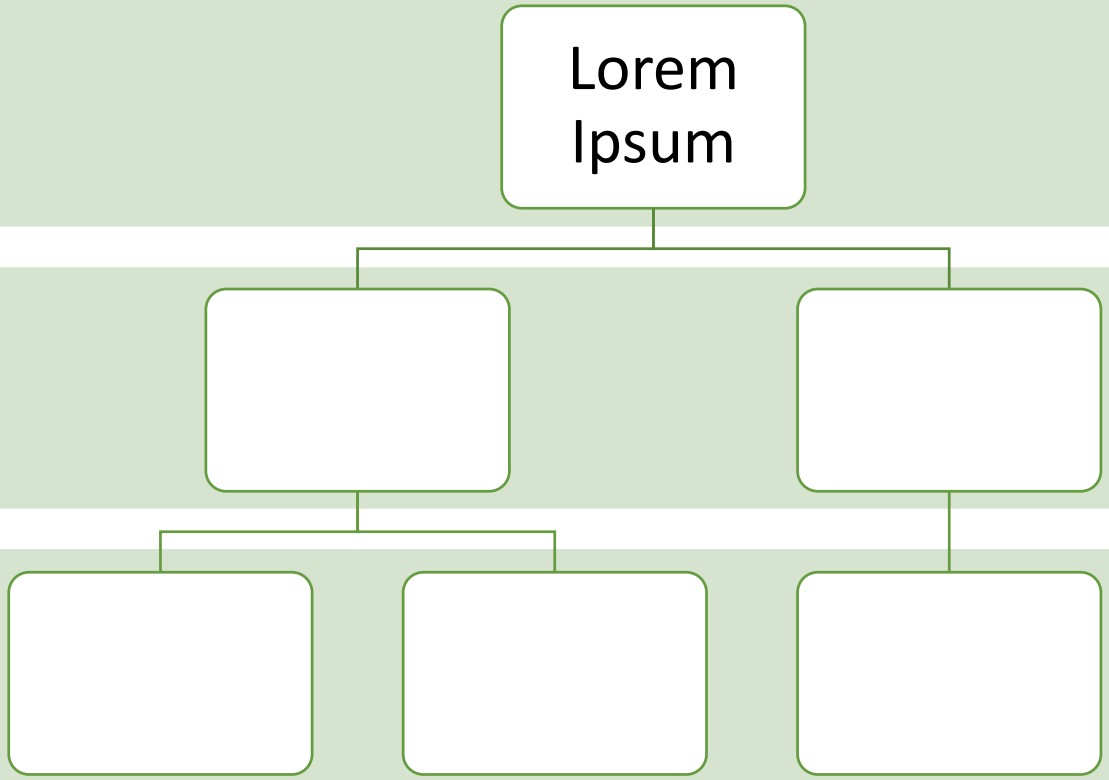

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

3RD ANNUAL NATIONAL
CYBERSECURITY
SUMMIT

LOREM IPSUM

LOREM IPSUM

LOREM IPSUM




CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
3RD ANNUAL NATIONAL
CYBERSECURITY
SUMMIT

How’d I do?

- Survey Monkey Link

- Mobile Link
  - Text Survey to XXX-XXX