



3<sup>RD</sup> ANNUAL NATIONAL  
**CYBERSECURITY  
SUMMIT**



# Recommended Cybersecurity Practices for Industrial Control Systems



3<sup>RD</sup> 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.

**Recommended Cybersecurity Practices for Industrial Control Systems**

**CYBERSECURITY CONSIDERATIONS**  
Industrial Control Systems (ICS) are important to supporting US critical infrastructure and maintaining national security. ICS owners and operators face threats from a variety of adversaries whose intentions include gathering intelligence and disrupting National Critical Functions. As ICS owners and operators adopt new technologies to improve operational efficiencies, they should be aware of the additional cybersecurity risk of connecting operational technology (OT) to enterprise information technology (IT) systems and Internet of Things (IoT) devices.

**Among the risks are:**

- Connecting ICS to external services, 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 accessibility to IT connectivity hardware and software, which can lead to a potential disruption of physical processes.

**CYBERSECURITY EVENT IMPACTS**

**SHORT-TERM IMPACTS**

- Operational downtime
- Loss of critical asset production and safety systems
- Potential loss due to equipment and hardware
- Intellectual property theft
- Health and safety system issues
- Damage and destruction of property and equipment
- Loss of availability
- Loss of control
- Data loss

**LONG-TERM IMPACTS**

- Significant operational losses, economic, and civil consequences
- Increased or denied resources
- Degraded equipment performance and quality
- Fees and penalties due to regulatory non-compliance
- Loss of customer
- Reduction of operational expenditure toward recovery efforts

**PRINCIPLES-LED DESIGN**

**CISA ASSESSMENTS: FISCAL YEAR 2019 MOST PREVALENT IT AND OT WEAKNESSES AND RISKS**

| Boundary Protection   | Principle of Least Functionality                                     | Identification and Authentication   | Physical Access Control   | Account Management                                      |
|---|--|---|---|---|
| <b>RISK:</b> Increased untrusted access to critical systems       | <b>RISK:</b> Increased access to critical systems                    | <b>RISK:</b> Loss of availability and integrity of critical systems   | <b>RISK:</b> Increased opportunity for equipment and information tampering  | <b>RISK:</b> Increased opportunity for account takeover |
| <b>RISK:</b> Weaker boundaries between ICS and enterprise systems | <b>RISK:</b> Opportunity for higher network access to be established | <b>RISK:</b> Increased difficulty in locating accounts to prevent loss of operations, especially sensitive to users with administrator access | <b>RISK:</b> Increased physical access to field equipment and information opportunities to: <ul style="list-style-type: none"> <li>• Manually modify devices or tags</li> <li>• Access the ICS network</li> <li>• Install malicious cyber agents</li> <li>• Add user devices to capture and exfiltrate network traffic</li> </ul> | <b>RISK:</b> Increased opportunity for account takeover |

**PROACTIVELY PROTECT TOMORROW**

| RISK MANAGEMENT AND CYBERSECURITY GOVERNANCE  | PHYSICAL SECURITY  | ICS NETWORK ARCHITECTURE   | ICS NETWORK PERIMETER SECURITY   |
|---|--|--|--|
| <ul style="list-style-type: none"> <li>• Identify threats to the organization</li> <li>• Maintain ICS asset inventory of all hardware, software, and supporting infrastructure technologies</li> <li>• Develop cybersecurity policies, procedures, training and educational materials that apply to organization's ICS</li> <li>• Develop and practice incident response procedures that join IT and OT response processes</li> </ul> | <ul style="list-style-type: none"> <li>• Lock down field electronics and set up alerting mechanisms for device manipulation such as power removal, device resets, and cabling changes</li> <li>• Ensure only authorized personnel have access to controlled spaces that house ICS equipment</li> <li>• Use multi-factor authentication, guards, and barriers to control logical and physical access to ICS equipment and facilities</li> </ul> | <ul style="list-style-type: none"> <li>• Utilize segmentation of networks where possible</li> <li>• Implement a network topology for ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer</li> <li>• Use one-way communication (scopes to prevent return traffic) for ICS equipment</li> <li>• Set up demilitarized zones (DMZ) to create a physical and logical demarcation that acts as an intermediary for connected security devices to avoid exposure</li> <li>• Employ reliable and secure network protocols and services where feasible</li> </ul> | <ul style="list-style-type: none"> <li>• Configure firewalls to control traffic between the ICS network and corporate IT network</li> <li>• Utilize IP geo-blocking as appropriate</li> <li>• Harden the remote access process to reduce risk to an acceptable level</li> <li>• Use jump servers as a central authorization location between ICS network security zones</li> <li>• Do not allow remote persistent vendor or employee connection to the control network</li> <li>• Catalog and monitor all remote connections to the network</li> </ul> |

| HOST SECURITY  | SECURITY MONITORING   | SUPPLY CHAIN MANAGEMENT  | HUMAN ELEMENT  |
|--|---|--|--|
| <ul style="list-style-type: none"> <li>• Promote a culture of patching and vulnerability management</li> <li>• Test all patches in offline test environments before implementation</li> <li>• Implement application whitelisting on human machine interfaces</li> <li>• Harden field devices, including tablets and smart phones</li> <li>• Replace out-of-date software and hardware devices</li> <li>• Disable unused ports and services on ICS devices after testing to ensure this will not impact ICS operation</li> <li>• Implement and test system backups and recovery processes</li> <li>• Configure encryption and security for ICS protocols</li> </ul> | <ul style="list-style-type: none"> <li>• Measure the baseline of normal operations and network traffic for ICS</li> <li>• Configure Intrusion Detection Systems (IDS) to create alarms for any ICS network traffic outside normal operations</li> <li>• Trace and monitor audit trails on critical areas of ICS</li> <li>• Set up Security Incident and Event Monitoring (SIEM) to monitor, analyze, and correlate event logs from across the ICS network to identify intrusion attempts</li> </ul> | <ul style="list-style-type: none"> <li>• Adjust ICS procurement process to weigh cybersecurity heavily as part of the bidding and evaluation methodology</li> <li>• Invest up front in secure ICS products, evaluating security against current and future threats over the product's product lifespan</li> <li>• Establish contractual agreements for all outsourced services that ensure proper incident handling and reporting, security of interconnections, and remote access authorizations and procedures</li> <li>• Consider ICS information integrity, security, and confidentiality when contracting with a cloud service provider</li> <li>• Leverage test labs to test uncontrolled software for malicious code and defects before implementation</li> </ul> | <ul style="list-style-type: none"> <li>• Issue policies that outline ICS security rules, including expected rules of behavior and required controls</li> <li>• Have procedures that state how personnel should manage ICS in a secure manner</li> <li>• Train IT operators, OT operators, and security personnel to recognize the indicators of potential compromise and what steps they should take to ensure that a cyber investigation succeeds</li> <li>• Promote a culture of dialogue and information exchange between security, IT, and OT personnel</li> </ul> |

**Defend ICS Processes Today**

- ✓ 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.

For additional information, including national alerts and recommendations, please visit CISA's Industrial Control Systems website: <https://www.cisa.gov/ics>

For additional information on the Department of Energy (DOE) cybersecurity initiatives, please visit: <https://www.energy.gov/energy-security>

# ICS Cyber Infographic Purpose

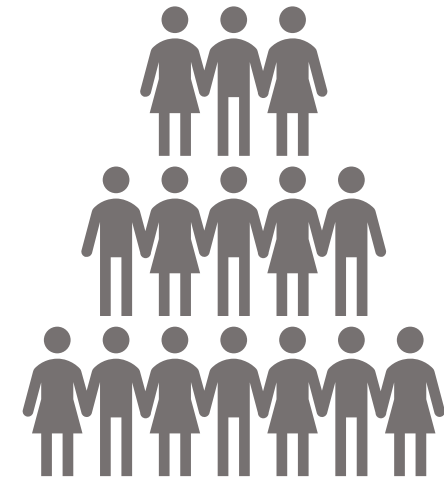
Call attention to the importance of ICS to critical infrastructure and start a conversation about proactive measures to defend ICS from cyber attacks

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)



## Boundary Protection



### RISK

Undetected unauthorized activity in critical systems



### RISK

Weaker boundaries between ICS and enterprise systems



## Identification and Authentication



### RISK

Lack of accountability and traceability for user actions if an account is compromised



### RISK

Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access



## Principle of Least Functionality



### RISK

Increased vectors for malicious party access to critical systems



### RISK

Opportunity for rogue internal access to be established



## Physical Access Control



### RISK

Unauthorized physical access to field equipment provides increased opportunity to:

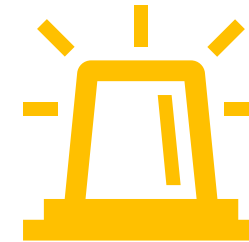
- Maliciously modify, delete, or copy device programs and firmware
- Access the ICS network
- Steal or vandalize cyber assets
- Add rogue devices to capture and retransmit network traffic



# 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:



**RISK MANAGEMENT  
AND CYBERSECURITY  
GOVERNANCE**



**PHYSICAL SECURITY**



**ICS NETWORK  
ARCHITECTURE**



**ICS NETWORK  
PERIMETER SECURITY**



**HOST SECURITY**



**SECURITY  
MONITORING**



**SUPPLY CHAIN  
MANAGEMENT**

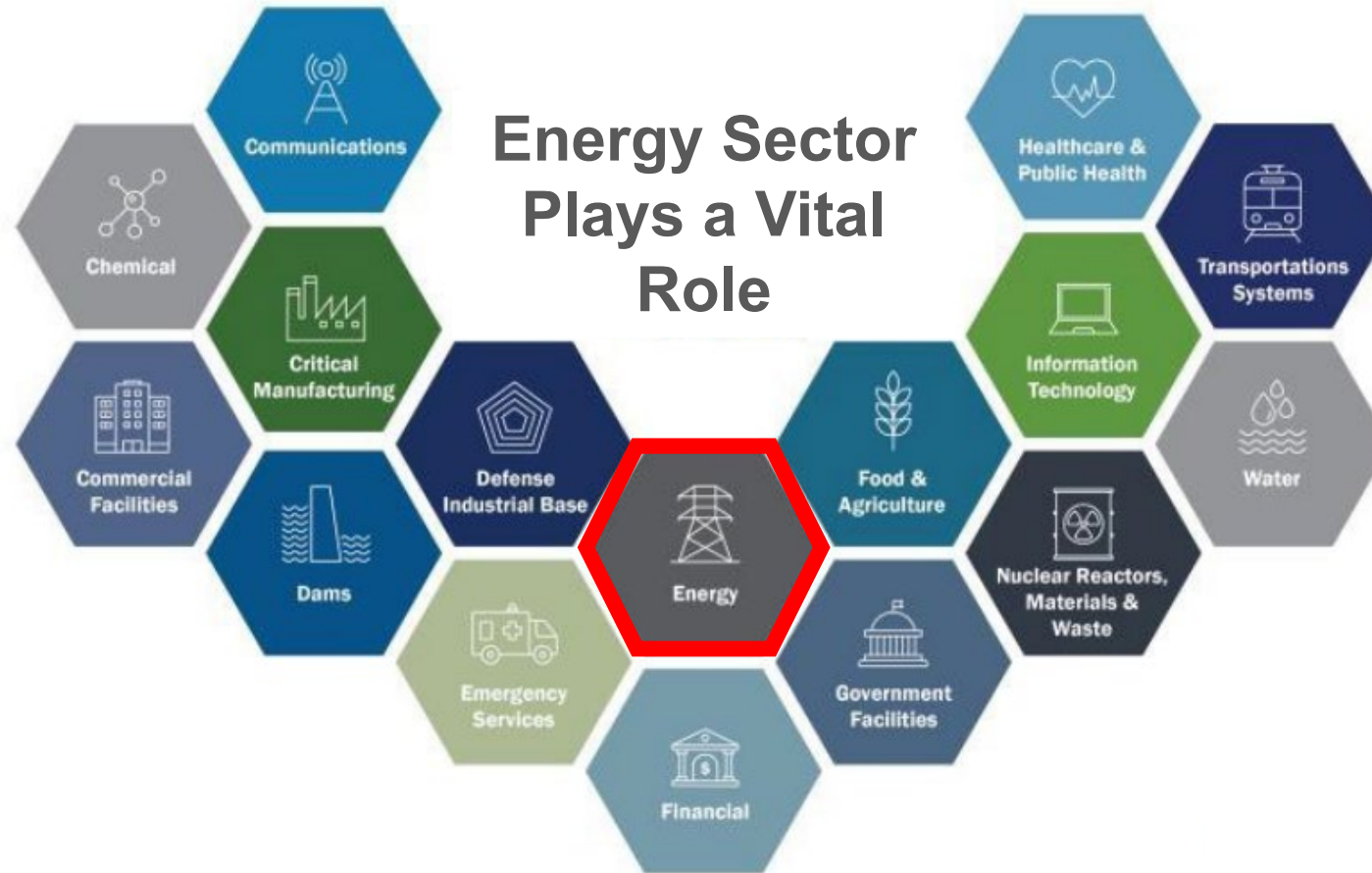


**HUMAN ELEMENT**



3<sup>RD</sup> ANNUAL NATIONAL  
**CYBERSECURITY  
SUMMIT**

# 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

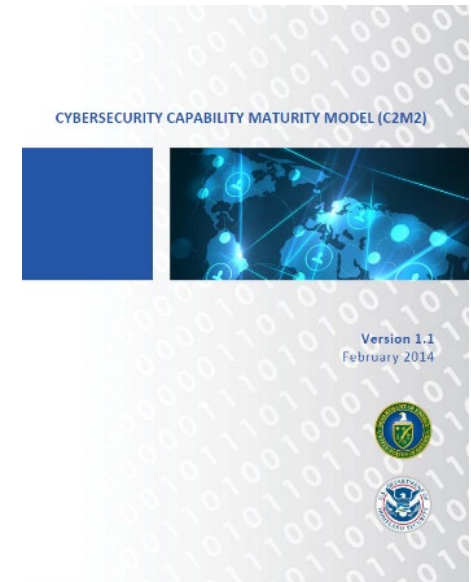


# Cybersecurity Capability Maturity Model (C2M2)

**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.







3<sup>RD</sup> ANNUAL NATIONAL  
**CYBERSECURITY  
SUMMIT**

**LOREM IPSUM**

Lorem  
Ipsum

**LOREM IPSUM**

**LOREM IPSUM**







3<sup>RD</sup> ANNUAL NATIONAL  
**CYBERSECURITY  
SUMMIT**

# How'd I do?

- Survey Monkey Link
- Mobile Link
  - Text Survey to XXX-XXX

