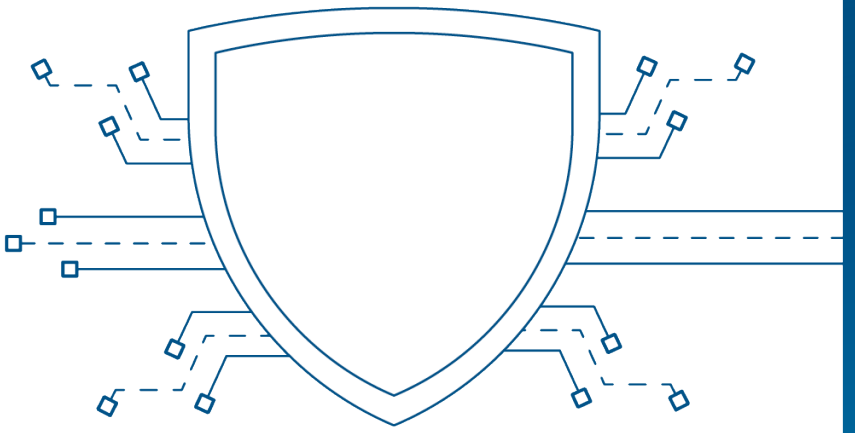
CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity Mission



CISA's Cybersecurity Division leads the national effort to reduce the prevalence and impact of cyber incidents by providing services, guidance, and capabilities that address immediate risks and advance toward a secure cyber ecosystem.

HOW CISA IS CARRYING OUT ITS CYBERSECURITY MISSION:

- Catalyze Persistent Collaboration Across Government and the Private Sector
- Expand Operational Visibility into Threats and Vulnerabilities
- Drive Prioritization and Measure Adoption of the Most Effective Security Measures
- Serve as the Operational Lead for Federal Civilian Cybersecurity
- Advance a Technology Product Ecosystem that is Secure by Design

State of Cybersecurity

Many organizations provide essential services that support the operation of all U.S. critical infrastructure. These critical organizations rely on information technology (IT) and sometimes operational technology (OT) systems to operate, and a compromise of these systems could lead to disruptions of service and significant cascading impacts throughout U.S. critical infrastructure.

Risks

Information Technology (IT) Systems

DATA

RANSOMWARE

IT/OT Convergence

NETWORK SEGMENTATION

Operational Technology (OT)

NETWORK COMPLEXITY

SYSTEM MAINTENANCE

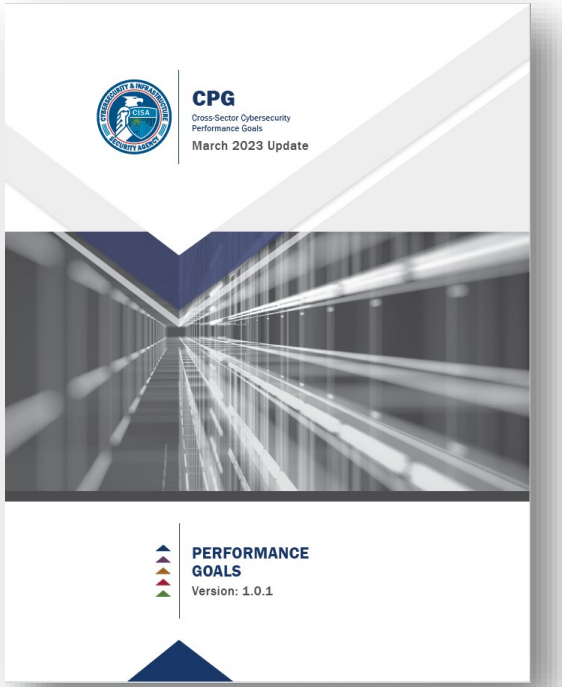
Preparedness Activities

Top Cyber Actions for Securing Systems

1. Reduce Exposure to the Public-Facing Internet
2. Conduct Regular Cybersecurity Assessments
3. Change Default Passwords Immediately
4. Conduct an Inventory of OT/IT Assets
5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans
6. Backup OT/IT Systems
7. Reduce Exposure to Vulnerabilities
8. Conduct Cybersecurity Awareness Training

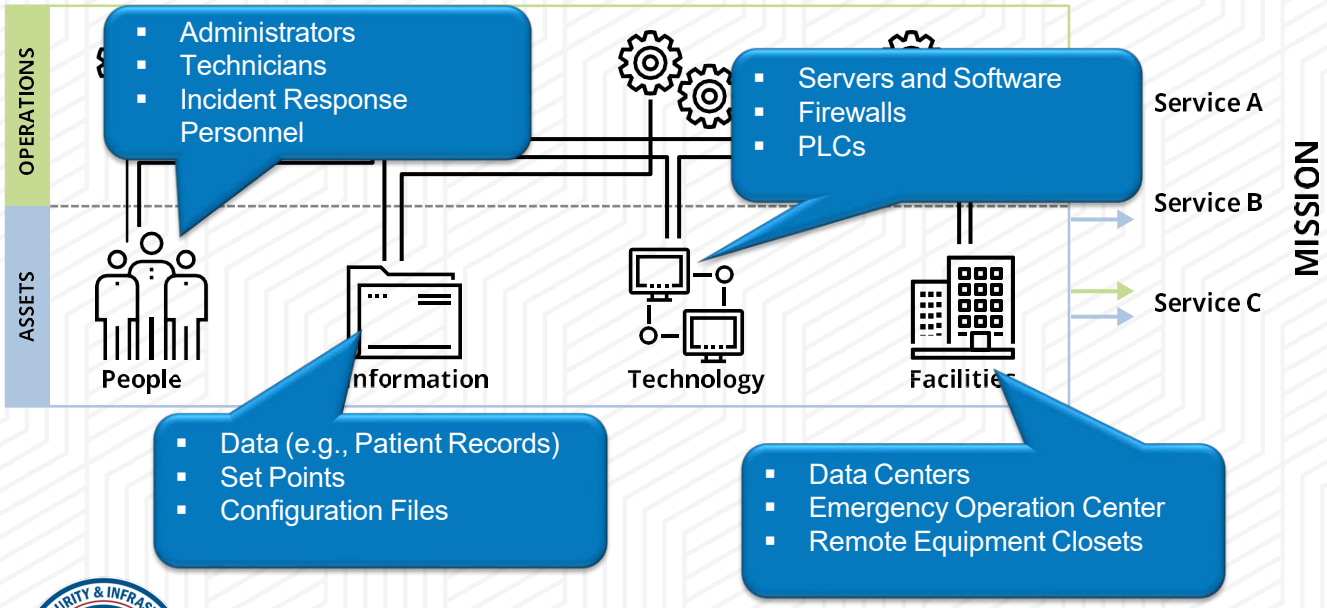
Ask your vendors how they are adopting cybersecurity principles within their services they provide you to mitigate threats!!!!!

Cross-Sector Cybersecurity Performance Goals (CPG)



- Interview-based assessment of baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value:
  - Align to the NIST CSF functions of Identify, Protect, Detect, Respond, Recover (38 Questions)
  - 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.
    - Available as: **CSA-facilitated**, or **self-assessment**
    - When facilitated, 2-person teams *(mastery level can conduct solo)*
  - **1-2** hours to complete and can be combined with a SAFE Assessment
  - CRR report

Asset Management



An organization uses its assets to perform productive activities to provide operational services and accomplish its mission.

Vulnerability Scanning by CISA

Known exploited vulnerabilities are easy access for attackers, with **incidents averaging $100,000 in damages** for small and medium businesses.

CISA's free vulnerability scanning service helps **identify exposed assets and exploitable vulnerabilities** and is proven to reduce risk for participating organizations.

Avoid costly disruptions with early detection and action. Through weekly reports and timely alerts, we will help you **act before others take advantage**.

BY THE NUMBERS

- **7,200+** current customers nationwide
- **Over 3 Million** vulnerabilities found and fixed
- On average a **40% reduction in risk and exposure** by newly enrolled customers in their first 12 months
- Most enrollees see improvements within the first **90 days**

GETTING STARTED

Email vulnerability@cisa.dhs.gov
Subject: "Requesting Vulnerability Scanning Services"

Segment and segregate OT from all other networks – Keep the back door shut.

FIGURE 1: UNSEGMENTED IT AND OT NETWORK

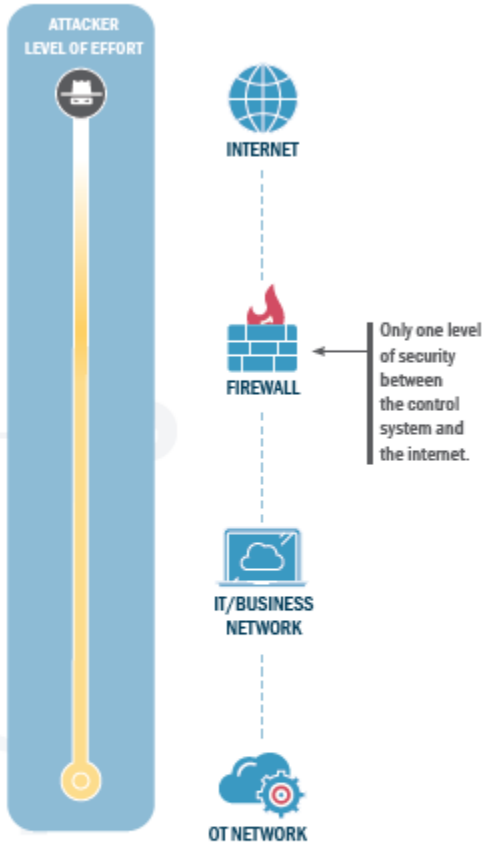
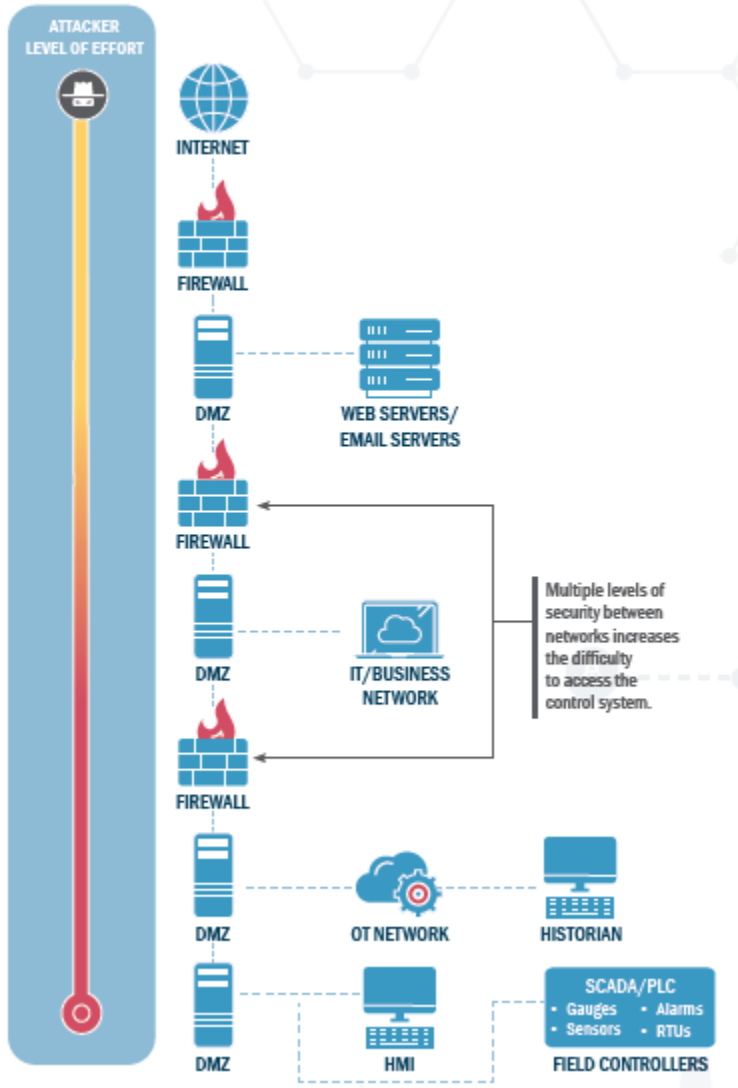
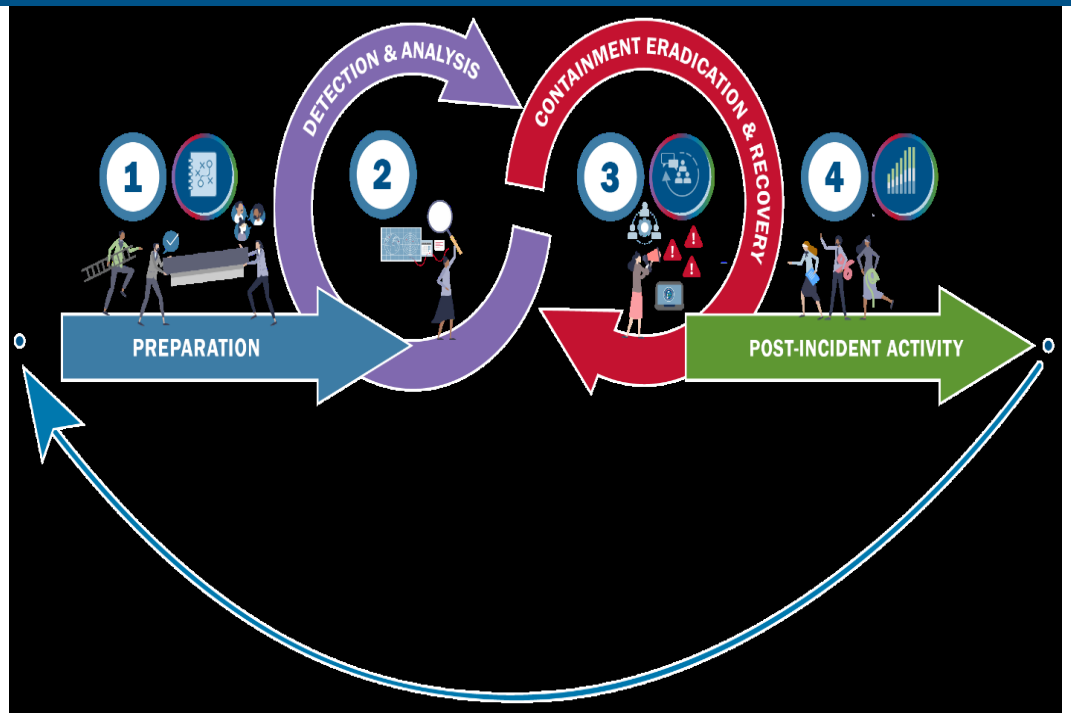


FIGURE 2: A SEGMENTED PURDUE ENTERPRISE REFERENCE ARCHITECTURE (PERA) NETWORK ARCHITECTURE



Responding Activities

- **Validate:** unusual behaviors, phishing attempts, unexplained data loss.
  - Disconnect compromised devices
- **Report:** vendor, MSP, and/or insurance company. State and Federal level reporting.
  - Document key information on the incident



Execute the utility ERP as needed, including notification of utility personnel, actions to restore operations of mission critical processes (e.g., switch to manual operation if necessary), and public notification (if required).

Incident Response Basics:
https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

IMR Training Series

The Identify, Mitigate, and Recover (IMR) incident response curriculum provides a range of training offerings encompassing cybersecurity awareness and best practices for organizations, live red/blue team network defense demonstrations emulating real-time incident response scenarios, and hands-on cyber range training courses for incident response practitioners.

Topics for Awareness Webinars & Cyber Range Training:

- Ransomware
- Cloud Security
- Business Email Compromise
- Vulnerabilities of Internet-Accessible Systems
- Web and Email Server Attacks
- DNS Infrastructure Attacks
- High Value Assets/Critical Assets
- Indicators of Compromise
- Incident Analysis with tool demo
- Investigating logs for incidents

Topics for Cyber Range Challenges & Observe the Attack Series:

- Ransomware
- Cloud Security
- Business Email Compromise

For more information, email: education@cisa.dhs.gov
Or visit: https://www.cisa.gov/incident-response-training

TLP: GREEN

Cyber Exercise & Planning Program

CISA designs, develops, conducts, and evaluates cyber exercises ranging from small-scale, limited scope, discussion-based exercises to large-scale, internationally-scoped, operations-based exercises.

CISA offers the following services at no-cost on an as-needed and as-available basis:

- Cyber Storm Exercise (CISA's flagship national level cyber exercise)
- End-to-End Cyber Exercise Planning
- Cyber Exercise Consulting
- Cyber Planning Support
- Exercise-In-A-Box

RESOURCES AVAILABLE TO YOU

- ***AARP:*** The AARP provides specifics on internet safety, how to protect your privacy, and the most up-to-date virus protections.
- ***FBI:*** This is a list of common fraud schemes aimed at older Americans.
- ***SeniorNet.org:*** SeniorNet offers computer training at senior centers, public libraries, schools, and hospitals as part of their mission to provide older adults computer technology education.
- ***Fraud.org*:** Fraud.org helps protect consumers from being victimized by fraud.
- ***FTC's PassItOn Campaign***: The PassItOn Campaign enlists people 65 and older in an effort to recognize and report fraud and other scams. Topics include imposter scams, identity theft, charity fraud, health care scams, paying too much, and "you've won" scams.

Other Federal Reporting Resources

FBI 24x7 CyWatch: (855) 292-3937 or CyWatch@fbi.gov

FBI Cyber Complaint Center: www.ic3.gov

For individuals who are victims of an online/digital crime

Federal Trade Commission – reportfraud.ftc.gov

For individuals who are victims of bad business practices or taken advantage of by online companies

Identity Theft Resources – IdentityTheft.gov

For individuals who believe they may be victims of Identity Theft

Next Steps: Partnership Formation!

1. Engage with your CISA Cybersecurity Advisor for assessments and to discuss cybersecurity protective measures, contact: robert.Kaminski@mail.cisa.dhs.gov (Western PA) and Derek.mueller@mail.cisa.dhs.gov (Central PA)

2. Sign-up for CISA's cyber hygiene services https://www.cisa.gov/cyber-hygiene-services (i.e., vulnerability scanning and web application scanning)
3. If you're a local government or authority get a dot GOV domain https://get.gov/

4. Subscribe to the CISA Email Listing: www.cisa.gov/subscribe-updates-cisa

5. Become familiar with:
    1. "Small and medium size business cybersecurity" webpage https://www.cisa.gov/audiences/small-and-medium-businesses

Visit **CISA.gov** to learn more and see our mission in action at **cisa.gov/about/2024YIR**
or contact us at **central@cisa.dhs.gov**