ASF Auditoría Superior de la Federación

CÁMARA DE DIPUTADOS

On the development of Cybersecurity and Data Protection Guidelines

LOTA Talks on Cyber Security

Roberto Hernandez Rojas Valderrama, SAI Mexico

Agenda

- Motivations to develop the Guideline
- Review of the Guideline
- Conclusions

Motivations

- Review and organize multiple sources of information
  - Standards and best practices
  - SAIs Reports
  - Public reports
- Do not develop a “bible”
- Prioritize usefulness
  - References (updated)
  - Examples
  - Links
- Take in consideration different cybersecurity maturity of countries

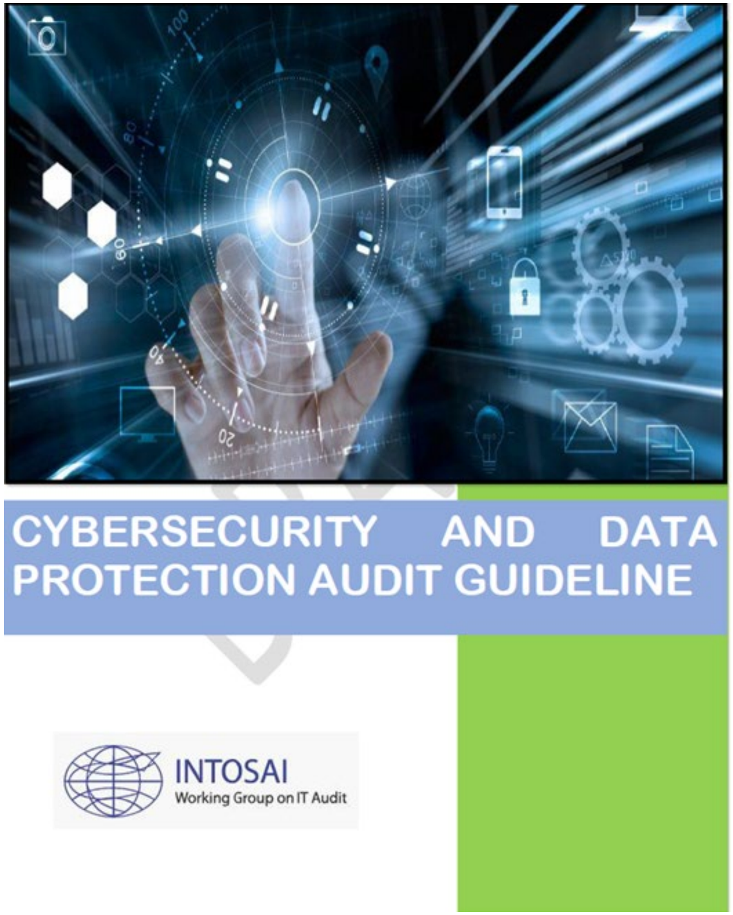
First approach

Introduction

Objective

1. Concepts and Definitions
2. Methodologies standards and frameworks
3. Guidance during audit phases
4. National Cybersecurity and data protection
5. Considerations of cybersecurity and data protection by sectors
6. Cybersecurity implications in relevant and emerging technologies
7. Tools and technical references

First approach



CYBERSECURITY AND DATA PROTECTION AUDIT GUIDELINE

INTOSAI
Working Group on IT Audit

Three-year Project
Participation of 10 SAIs

The finalized draft document was hosted on the WGITA website and was circulated to WGITA members in October 2022.

1. Introduction
2. Guidance during audit phases
3. Auditing national Cybersecurity and data Protection
4. Considerations of cybersecurity and data protection by sector

https://www.intosaicommunity.net/wgita/wp-content/uploads/2023/02/Cybersecurity_and_Data_Protection_Guideline-2022.pdf

Chapter 1 Introduction

Brief referral to **relevant** concepts, definitions, methodologies, standards and frameworks, related to Cybersecurity, Data protection and Data Privacy.

Lead	Member (s)
USA and India	Kuwait , Argentina and Mexico

Chapter 1 Introduction

- ISO/IEC 27000:2018
- Information technology security techniques
- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1
- NIST Special Publication 800-34: Revision 1, Contingency Planning Guide for Federal Information Systems
- NIST Special Publication (SP) 800-37, Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle
- NIST SP 800-55 Rev. 1: Performance Measurement Guide for Information Security
- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide
- NIST 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment NIST SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-161, Rev 1 (Final): Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 "appropriate technical and organizational measures."

Chapter 2 Guidance during audit phases

Includes audit guidance, how to start audits on cybersecurity and data protection (planning, execution, reporting, follow up, termination, file and disposal).

Lead	Member (s)
Australia	India and Japan

Chapter 2 Guidance during audit phases

The principles will provide guidelines on:

- Defining the terms of the engagement; and
- Defining the scope.

Risk-based Approach to Cyber Security	
Steps	Description
1. Define the system	Determine the type, value and security objectives for the system based on an assessment of the impact if it were to be compromised.
2. Select controls	Select controls for the system and tailor them to achieve desired security objectives.
3. Implement controls	Implement controls for the system and its operating environment.
4. Assess controls	Assess controls for the system and its operating environment to determine if they have been implemented correctly and are operating as intended.
5. Authorize the system	Authorize the system to operate based on the acceptance of the security risks associated with its operation.
6. Monitor the system	Monitor the system, and associated cyber threats, security risks and controls, on an ongoing basis.

Chapter 2 Guidance during audit phases

Audit Program Development

Audit Skill Requirements

(CISSP) (CISA) (CISM)
(CySA+) (CEH) (CRISC)
(GSEC)

Principles for conducting the following types of audits:

Cyber security capability/ maturity	Cyber security strategy Cyber security risk management Program management and governance Regulatory and legal requirements Threat and vulnerability management Security incident management Security Monitoring Workforce management Third-party management Data protection
Cyber resilience maturity	Business impact analysis Business continuity planning Disaster recovery planning Security incident management Threat and vulnerability management Security Monitoring Third-party management Workforce management
Data Protection	Data governance Regulatory and legal requirements Data classification Data security Data quality management Information records management Data loss prevention
Technical Configuration	Hardening standards Configuration management Security build and testing Development lifecycles Patch management Vulnerability management

Chapter 2 Guidance during audit phases

Reporting

Principles

- Information included in the report should be reviewed to determine whether it increases the cyber security risks to the organization and/or nation.
  - Information that is not publicly available should not be included in the report.
  - Names of systems, tools, staff and teams should be removed if possible.
  - Security information such as security monitoring processes, security configurations, and vulnerabilities should not be included in the report, and more importantly, connected to systems or organizations.
- The materiality of the information can be used to exclude information from the report
- The auditor can aim to aggregate and generalize security information to reduce the risks of security controls being attributed to specific systems.

Chapter 3 Auditing national cybersecurity and data protection

Provide SAIs with guidance (including relevant information such as the applicable framework when conducting such audit types), this section provides highlights on a) national and regional cybersecurity benchmark studies from global and regional organizations (APEC, ASEAN, LAS, OAS, PIF, SAARC, among others) and b) national cybersecurity considerations (UN, ENISA, NIST, ITU, among others) in terms of disaster recovery, Critical Infrastructure, National Cyber Incident Response

Lead	Member (s)
Mexico	China and Peru

Chapter 3 Auditing national cybersecurity and data protection

Three Dimensions	1. Governmental 2. National 3. International
The Five Mandates of National Cyber Security	1. Military Cyber 2. Counter Cyber Crime 3. Intelligence and Counter-Intelligence 4. Critical Infrastructure Protection and National Crisis Management 5. Cyber Diplomacy’ and Internet Governance
The Five Dilemmas of National Cybersecurity	1. Stimulate the Economy vs. Improve National Security. 2. Infrastructure Modernization vs. Critical Infrastructure Protection. 3. Private Sector vs. Public Sector. 4. Data Protection vs. Information Sharing. 5. Freedom of Expression vs. Political Stability.

Chapter 3 Auditing national cybersecurity and data protection

Characteristic	Definition	Required Information	Analysis
Purpose, scope, and methodology	Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.	Applicable policies, strategies, and laws to confirm the key federal entities with roles and responsibilities in supporting the nation's cybersecurity.	• "This plan was created to…" • "Purpose" statement • Executive summary
Problem definition and risk assessment	Addresses the national problems and threats the strategy is directed towards and entails a risk assessment that includes an analysis of threats, and vulnerabilities of, critical assets and operations.	A risk assessment that includes an analysis of threats, and vulnerabilities of critical assets and operations.	• Risk assessment, including an analysis of threats and vulnerabilities • Issue areas
Goals, subordinate objectives, activities, and performance measures	Addresses what the strategy is trying to achieve, steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.	Priorities, milestones, and performance measures to gauge results.	• Milestones for achieving goals • Performance measures for tracking progress • Reporting requirements • Life cycle/time frames • Standards
Resources, investments, and risk management	Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted based on balancing risk reductions with costs.	Cost analysis. Specific risks assessment.	• Analysis of the cost of planned activities • Estimates of how activities will be funded in the future • Source and type of resources needed to carry out the goals and objectives • Assessment of the specific risks and resources needed to mitigate them

Chapter 3 Auditing national cybersecurity and data protection

Characteristic	Definition	Required Information	Analysis
Organizational roles, responsibilities, and coordination	Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.	Relevant federal officials' interviews to confirm the key federal entities. Cybersecurity-related roles and responsibilities for each federal entity.	• Delegation of responsibilities • Oversight responsibilities • Clarity for individual agencies' response options to specific incidents • Coordination groups • "XX is responsible for…"/ "XX shall…" • "XX will do ___ by doing…"
Integration and implementation	Addresses how a national strategy relates to the goals, objectives, and activities of other strategies, and to subordinate levels of government and their plans to implement the strategy.	Applicable policies, strategies, and laws.	• How strategy is linked to or superseded by other documents and strategies • Describes progress made since previous strategies or plans • Why activities in this plan are prioritized differently than in other plans • Crosswalk(s)

Chapter 3 Auditing national cybersecurity and data protection

Auditing of Critical National Infraestructure	
General	Canada Turkey Australia Brazil
Semi-Specific	United Kingdom
Specific	United States of America

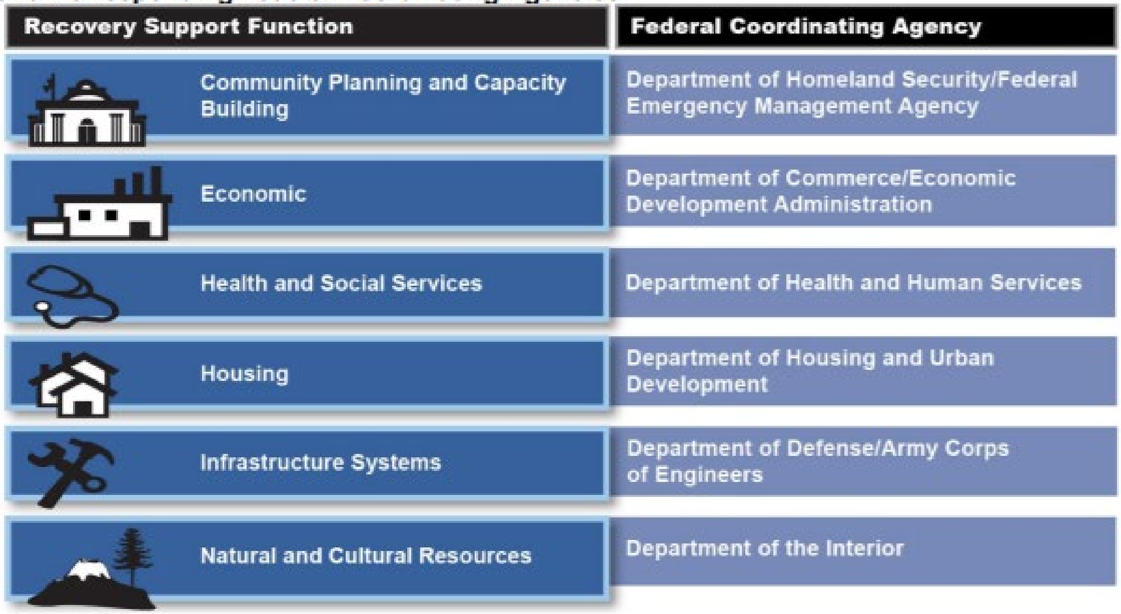
- Objective
- Scope and methodology
- Frameworks and Guides
- Conclusions
- Recommendations

Chapter 3 Auditing national cybersecurity and data protection

Auditing National Resilience / Disaster Recovery	
General	Australia Brazil
By Functions	United States of America

- Objective
- Scope and methodology
- Frameworks and Guides
- Conclusions
- Recommendations

The National Disaster Recovery Framework's Recovery Support Functions and Corresponding Federal Coordinating Agencies



Recovery Support Function	Federal Coordinating Agency
Community Planning and Capacity Building	Department of Homeland Security/Federal Emergency Management Agency
Economic	Department of Commerce/Economic Development Administration
Health and Social Services	Department of Health and Human Services
Housing	Department of Housing and Urban Development
Infrastructure Systems	Department of Defense/Army Corps of Engineers
Natural and Cultural Resources	Department of the Interior

Source: GAO analysis of Federal Emergency Management Agency (FEMA) information. | GAO-16-476

Chapter 3 Auditing national cybersecurity and data protection

Pillar-based assessment for cybersecurity agencies

Pillars	Description	Required Information	Elements to be evaluated	References Guides and Good practices
Foundations of CSIRT				
Organization				
Human Resources				
Tools				
Process				

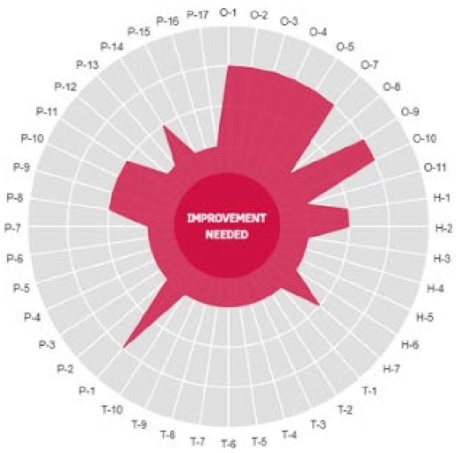
Chapter 3 Auditing national cybersecurity and data protection

Assessing the maturity level of a CSIRT

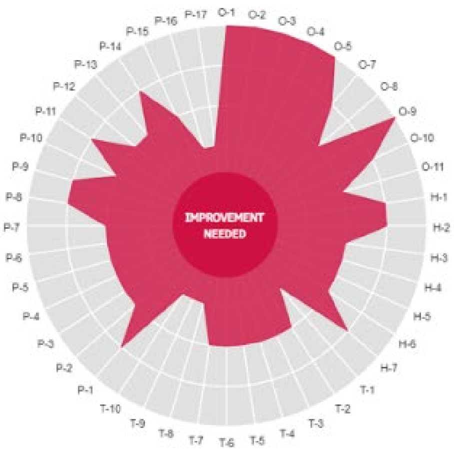
SIM 3 Model

Parameter	Number of questions
Organization	10
Human	7
Tools	10
Process	17

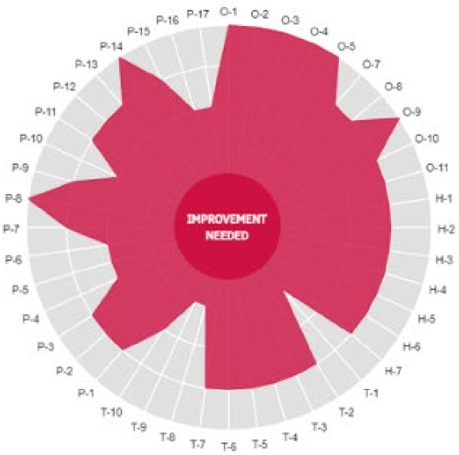
Basic Maturity



Intermediate Maturity



Advanced Maturity



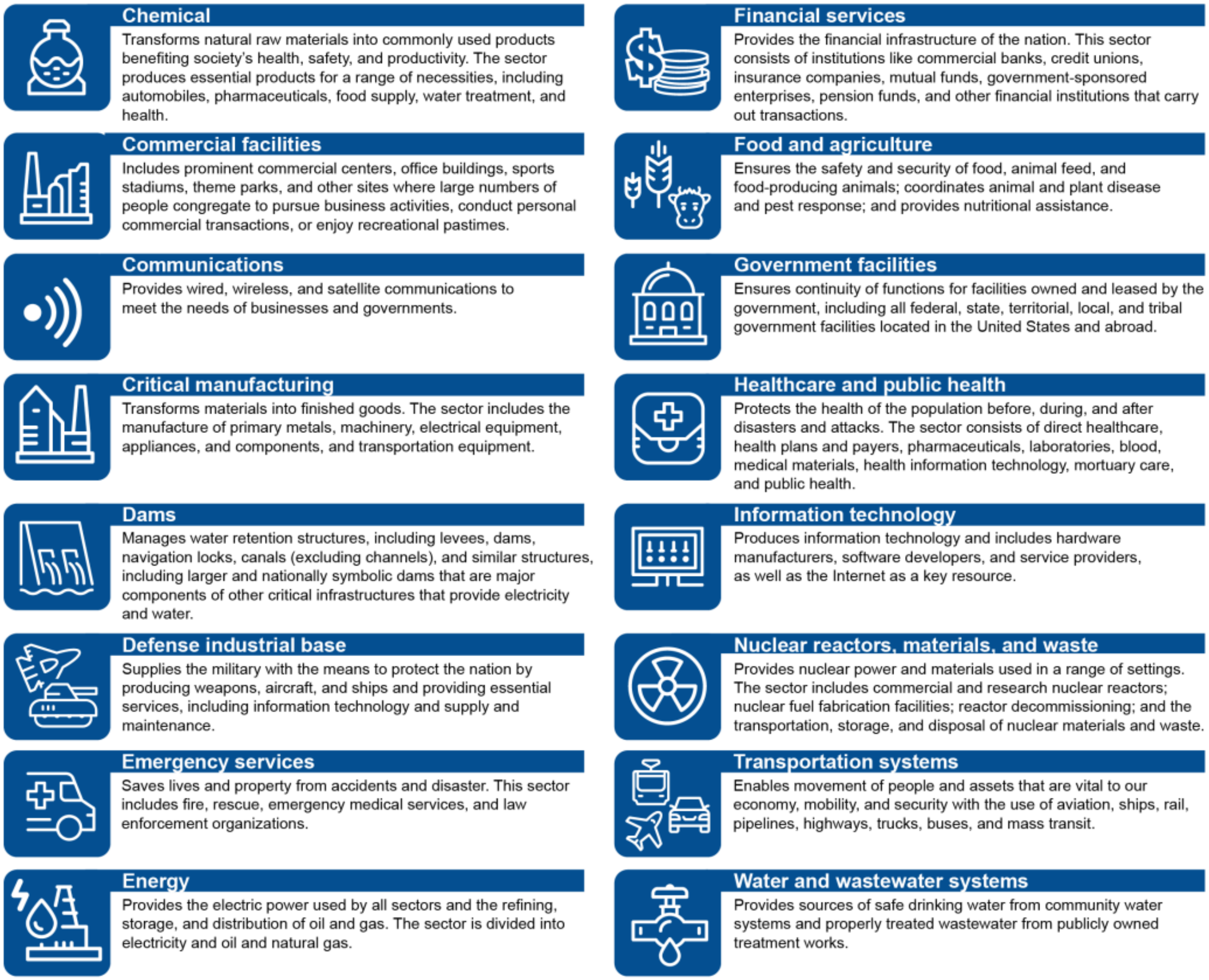
Chapter 4 Considerations of cybersecurity and data protection by sectors

Cybersecurity audits require SAIs to consider the different economic sectors governments are involved in.

Some examples include cybersecurity and data protection in the financial, energy, health care, telecommunications and e-commerce sectors.

Lead	Member (s)
USA	Bangladesh

Chapter 4 Considerations of cybersecurity and data protection by sectors



Chemical

Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The sector produces essential products for a range of necessities, including automobiles, pharmaceuticals, food supply, water treatment, and health.

Commercial facilities

Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.

Communications

Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.

Critical manufacturing

Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.

Dams

Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.

Defense industrial base

Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.

Emergency services

Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.

Energy

Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.

Financial services

Provides the financial infrastructure of the nation. This sector consists of institutions like commercial banks, credit unions, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.

Food and agriculture

Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.

Government facilities

Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.

Healthcare and public health

Protects the health of the population before, during, and after disasters and attacks. The sector consists of direct healthcare, health plans and payers, pharmaceuticals, laboratories, blood, medical materials, health information technology, mortuary care, and public health.

Information technology

Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.

Nuclear reactors, materials, and waste

Provides nuclear power and materials used in a range of settings. The sector includes commercial and research nuclear reactors; nuclear fuel fabrication facilities; reactor decommissioning; and the transportation, storage, and disposal of nuclear materials and waste.

Transportation systems

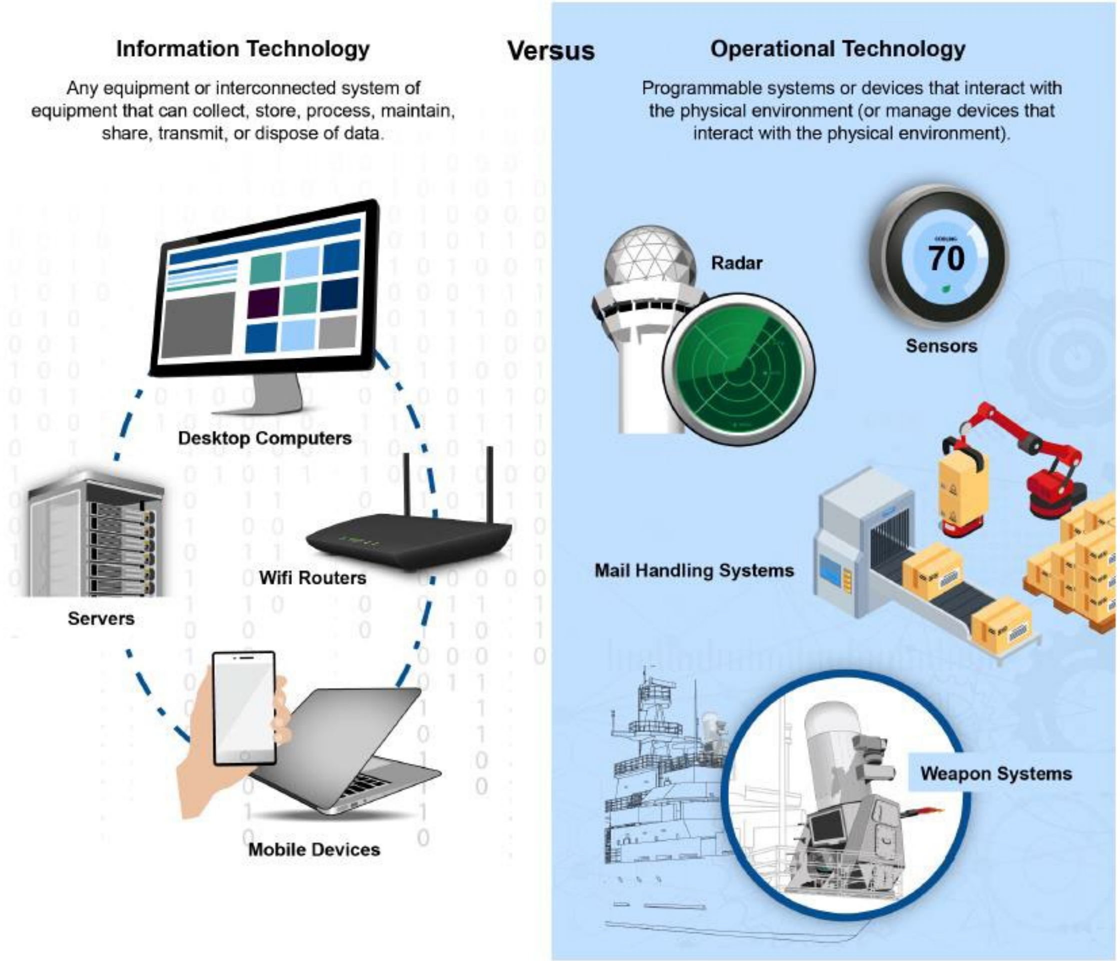
Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.

Water and wastewater systems

Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.

Source: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013; images: motorama/stock.adobe.com.

Chapter 4 Considerations of cybersecurity and data protection by sectors



Information Technology

Any equipment or interconnected system of equipment that can collect, store, process, maintain, share, transmit, or dispose of data.

Versus

Operational Technology

Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).

Source: GAO analysis of National Institute of Standards and Technology guidance and Coast Guard documentation; images: Vikivector/stock.adobe.com, kurtcan/stock.adobe.com, robu_s/stock.adobe.com, royyimzy/stock.adobe.com, Yevhenii/stock.adobe.com. | GAO-22-105092

Chapter 4 Considerations of cybersecurity and data protection by sectors

Common Methods of Intentional Cyber Exploits

- Exploit
- Watering hole
- Phishing and spear phishing
- Credentials based
- Trusted third parties
- Classic buffer overflow
- Cryptographic weakness
- Structured Query Language (SQL) injection
- Operating system command injection
- Cross-site scripting
- Cross-site request forgery
- Path traversal
- Integer overflow
- Uncontrolled format string
- Open redirect
- Heap-based buffer overflow
- Unrestricted upload of files
- Inclusion of functionality from untrusted sphere
- Certificate and certificate authority compromise
- Hybrid of others

Chapter 4 Considerations of cybersecurity and data protection by sectors

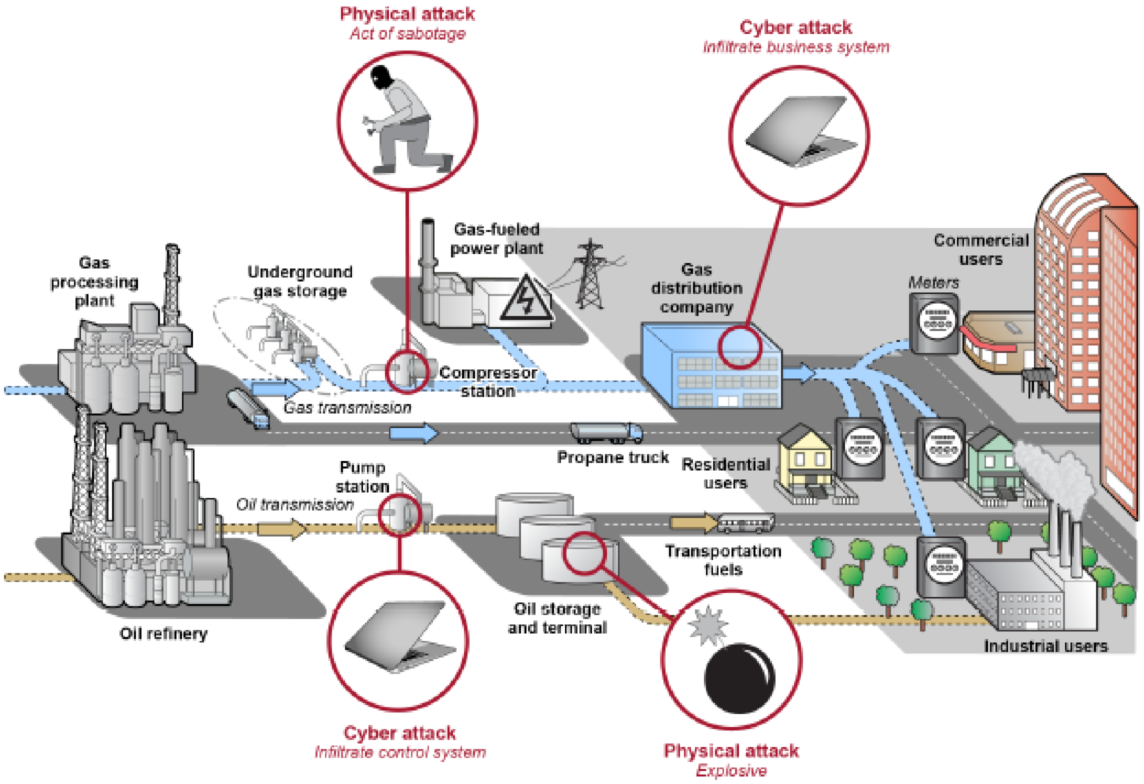
Examples of recent cybersecurity attacks on critical infrastructure sectors

Energy
Ukrainian Power Gird

Transportation
US – Colonial Pipeline

Communications
Viasat European satellite

Water and wastewater
US water treatment facilities



Source: GAO analysis of Transportation Security Administration information. | GAO-21-288

Conclusions

- Cybersecurity and data protection audit are multinational (people, process and technology)
- The guideline provides relevant information to each SAI according to the maturity in legislations, skills and resources
- The guideline requires a continuous (year) review and update
- It would be a general guideline that could be used with more detailed documentes, v.g. auditing cloud computing, emerging technologies

Thank You