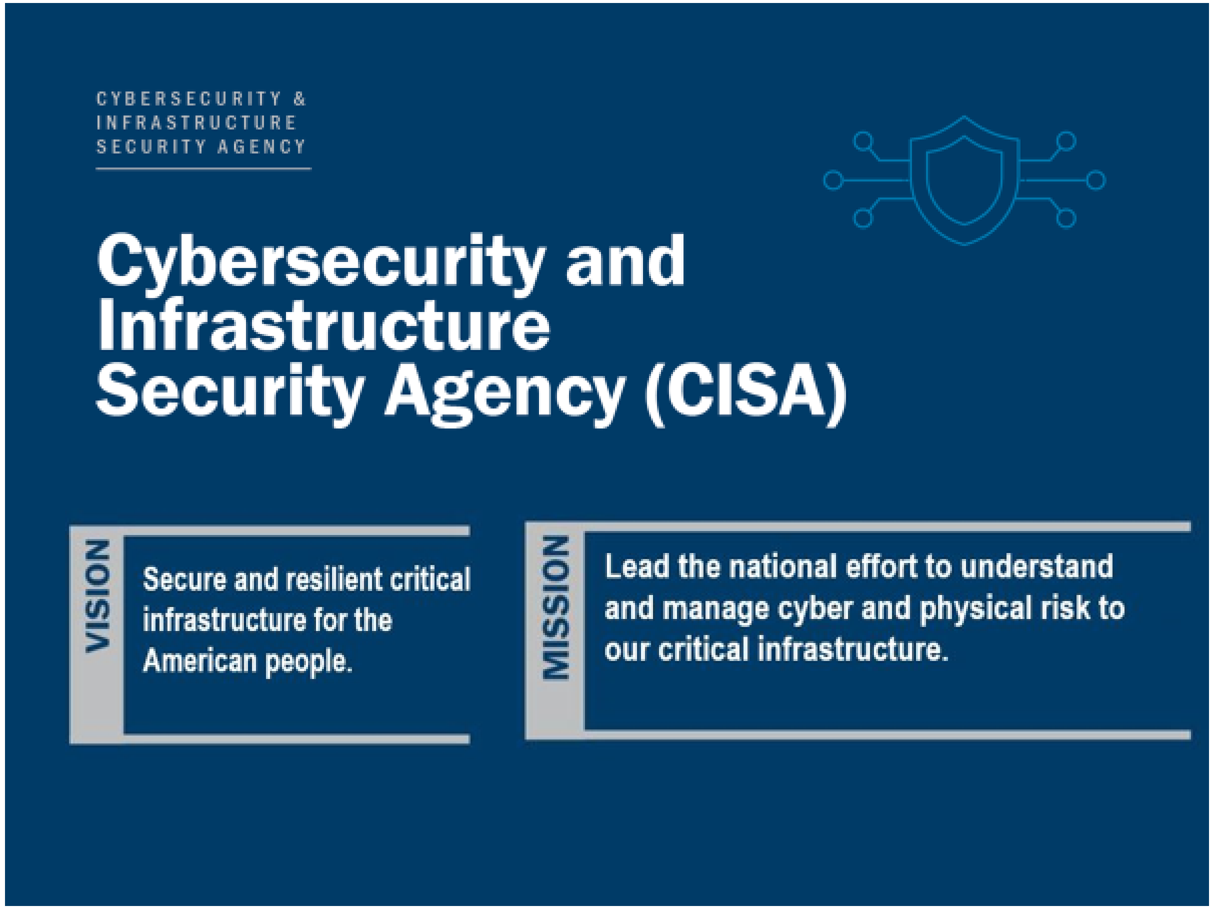
CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CYBER THREAT TO MANUFACTURING

CISA CYBERSECURITY SERVICES

Joe Parker
Cybersecurity Advisor, Region 4, Huntsville, AL
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency (CISA)

Critical Infrastructure Protection



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

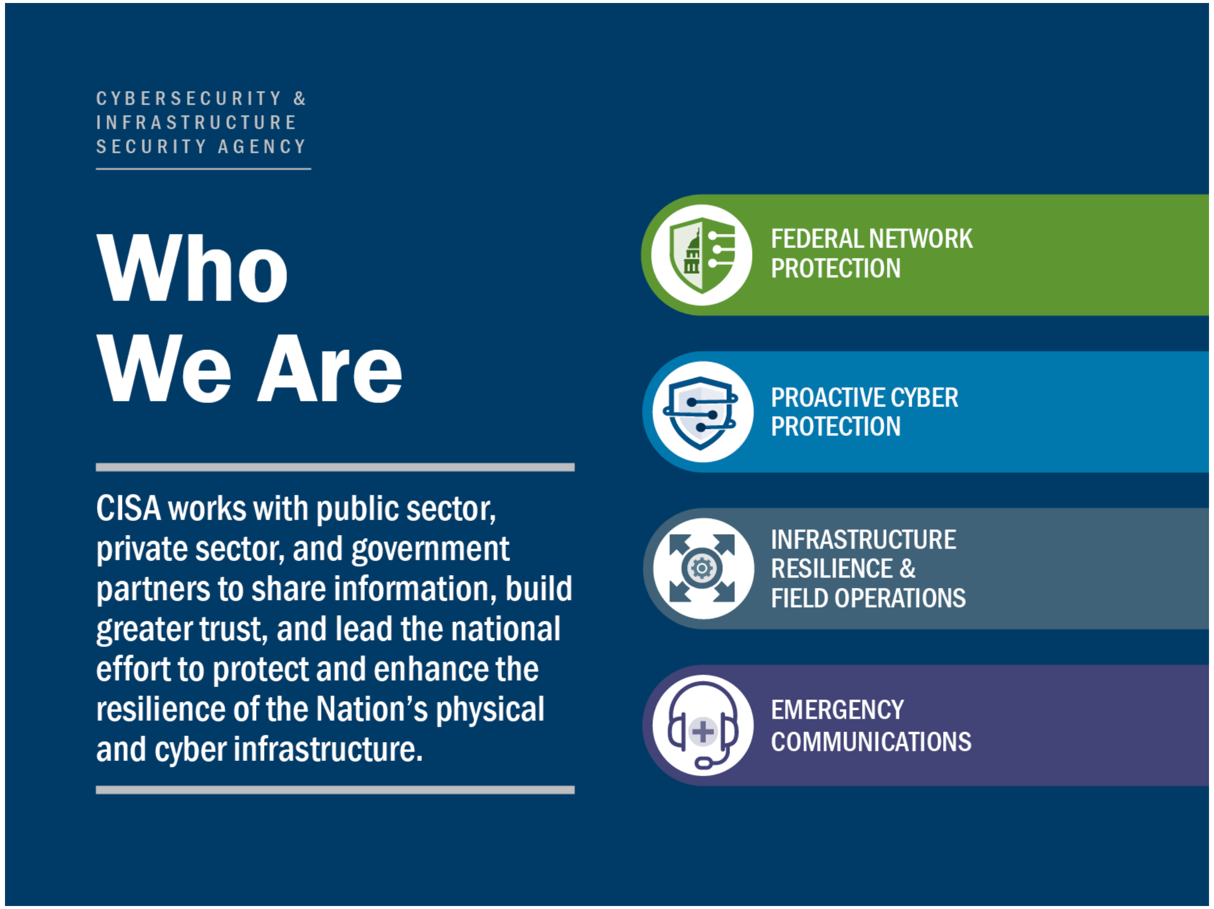
Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient critical infrastructure for the American people.

MISSION

Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.



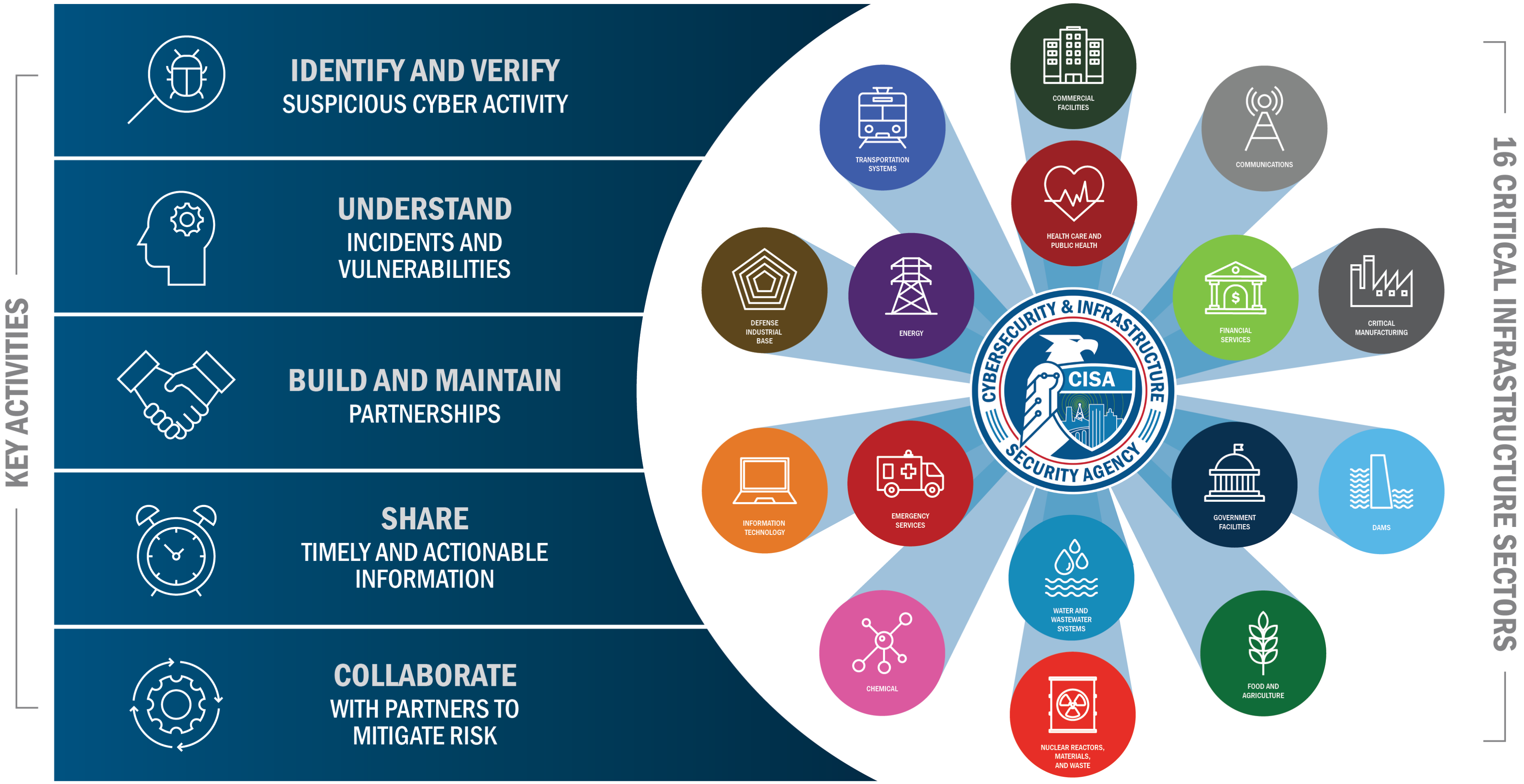
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

- FEDERAL NETWORK PROTECTION
- PROACTIVE CYBER PROTECTION
- INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
- EMERGENCY COMMUNICATIONS

CSAs-Serving Critical Infrastructure



KEY ACTIVITIES

IDENTIFY AND VERIFY
SUSPICIOUS CYBER ACTIVITY

UNDERSTAND
INCIDENTS AND VULNERABILITIES

BUILD AND MAINTAIN
PARTNERSHIPS

SHARE
TIMELY AND ACTIONABLE INFORMATION

COLLABORATE
WITH PARTNERS TO MITIGATE RISK

16 CRITICAL INFRASTRUCTURE SECTORS

- COMMERCIAL FACILITIES
- TRANSPORTATION SYSTEMS
- COMMUNICATIONS
- HEALTH CARE AND PUBLIC HEALTH
- DEFENSE INDUSTRIAL BASE
- ENERGY
- FINANCIAL SERVICES
- CRITICAL MANUFACTURING
- INFORMATION TECHNOLOGY
- EMERGENCY SERVICES
- GOVERNMENT FACILITIES
- DAMS
- WATER AND WASTEWATER SYSTEMS
- CHEMICAL
- FOOD AND AGRICULTURE
- NUCLEAR REACTORS, MATERIALS, AND WASTE

16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

CHEMICAL	DHS (CISA)
COMMERCIAL FACILITIES	DHS (CISA)
COMMUNICATIONS	DHS (CISA)
CRITICAL MANUFACTURING	DHS (CISA)
DAMS	DHS (CISA)
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	DHS (CISA)
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & DHS (FPS)
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	DHS (CISA)
NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
TRANSPORTATIONS SYSTEMS	(TSA & USCG)
WATER	EPA

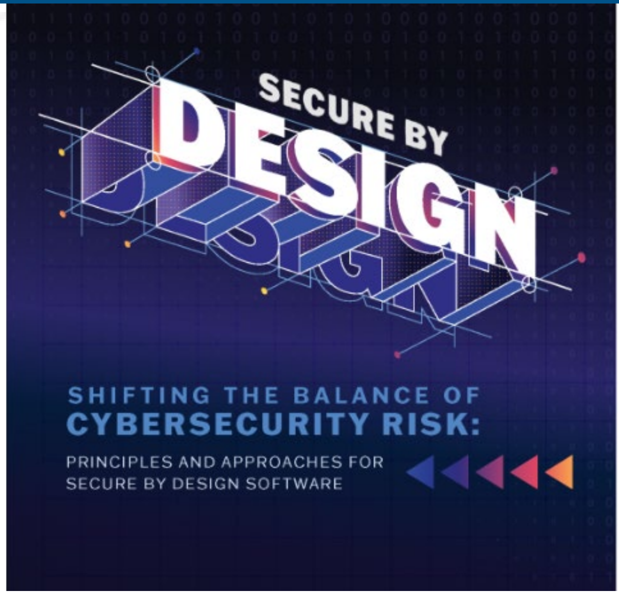
SECURE BY DESIGN
SECURE BY DEFAULT

The Problem

- **Customers Carrying the Burden**
  - Appling Patches Daily
  - Log Reviews
  - Buy Additional Security Products
  - Lengthy Hardening Guides
  - Identity Access Management
  - Etc...(we could easily go on, and on, and on…)

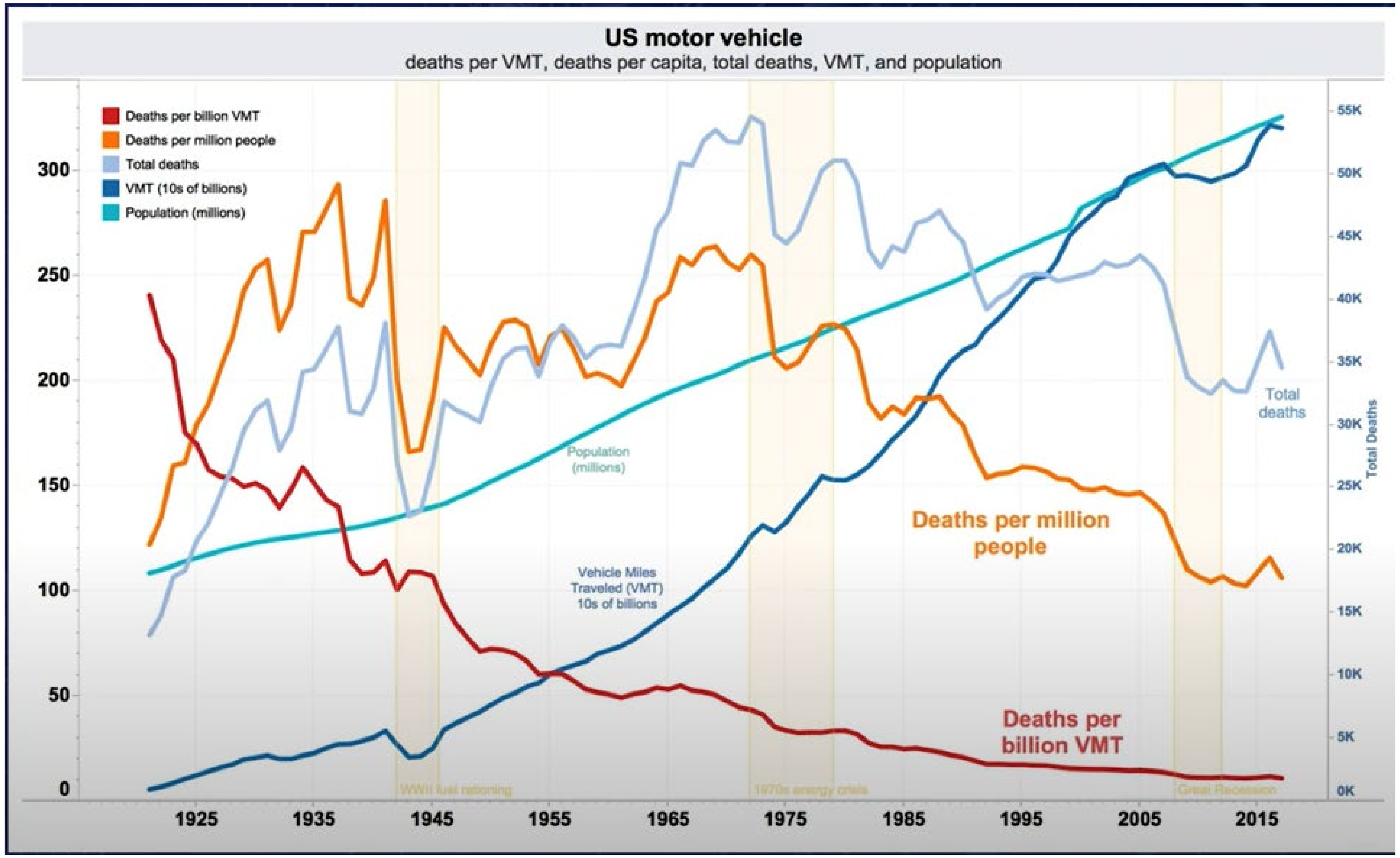
Global Call to Action

- **“Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software”**
  - 17 U.S. and International Partners, Co-Sealed by 8 International Cybersecurity Agencies
  - Shift the burden of security from least capable to most capable-manufactures



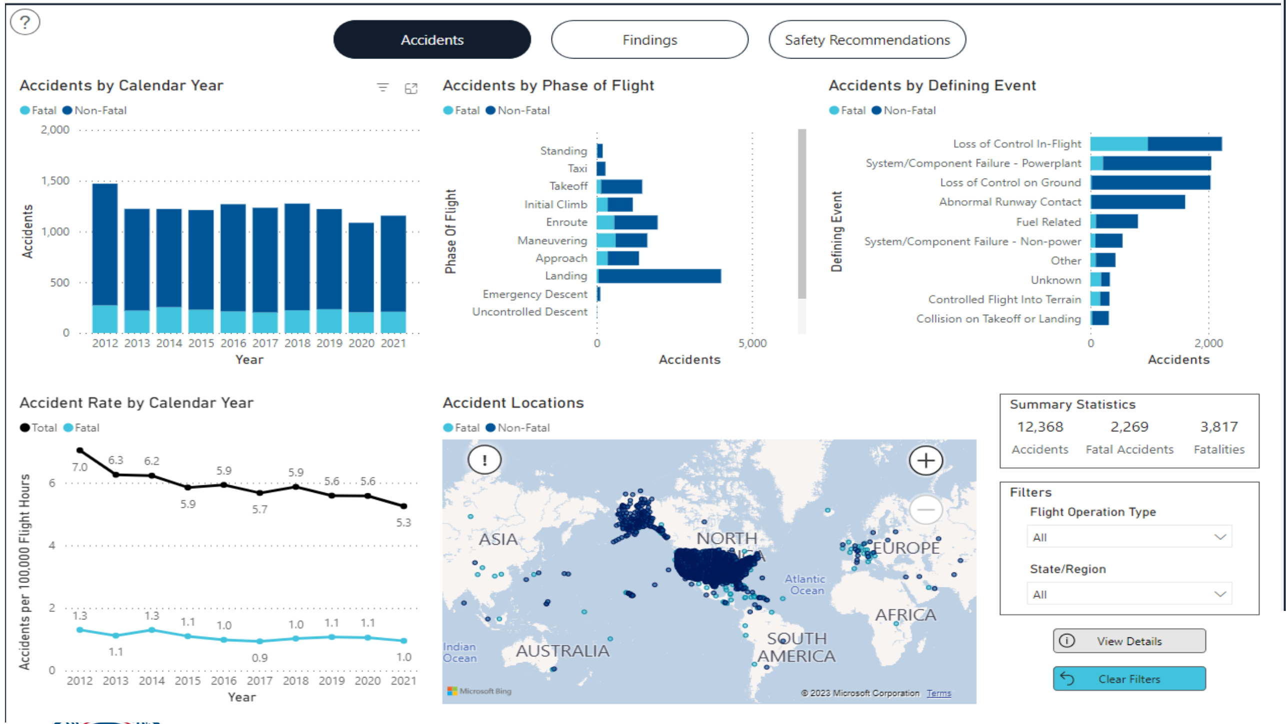
Mature Industries

- **Automotive Industry**
  - Population Increased
  - Vehicle Miles Traveled (VMT) Increased
  - Deaths per Billion VMT Decreased



Mature Industries

- **NTSB General Aviation Accident Dashboard**
  - Decrease in Accidents
  - **Root Cause Analysis**



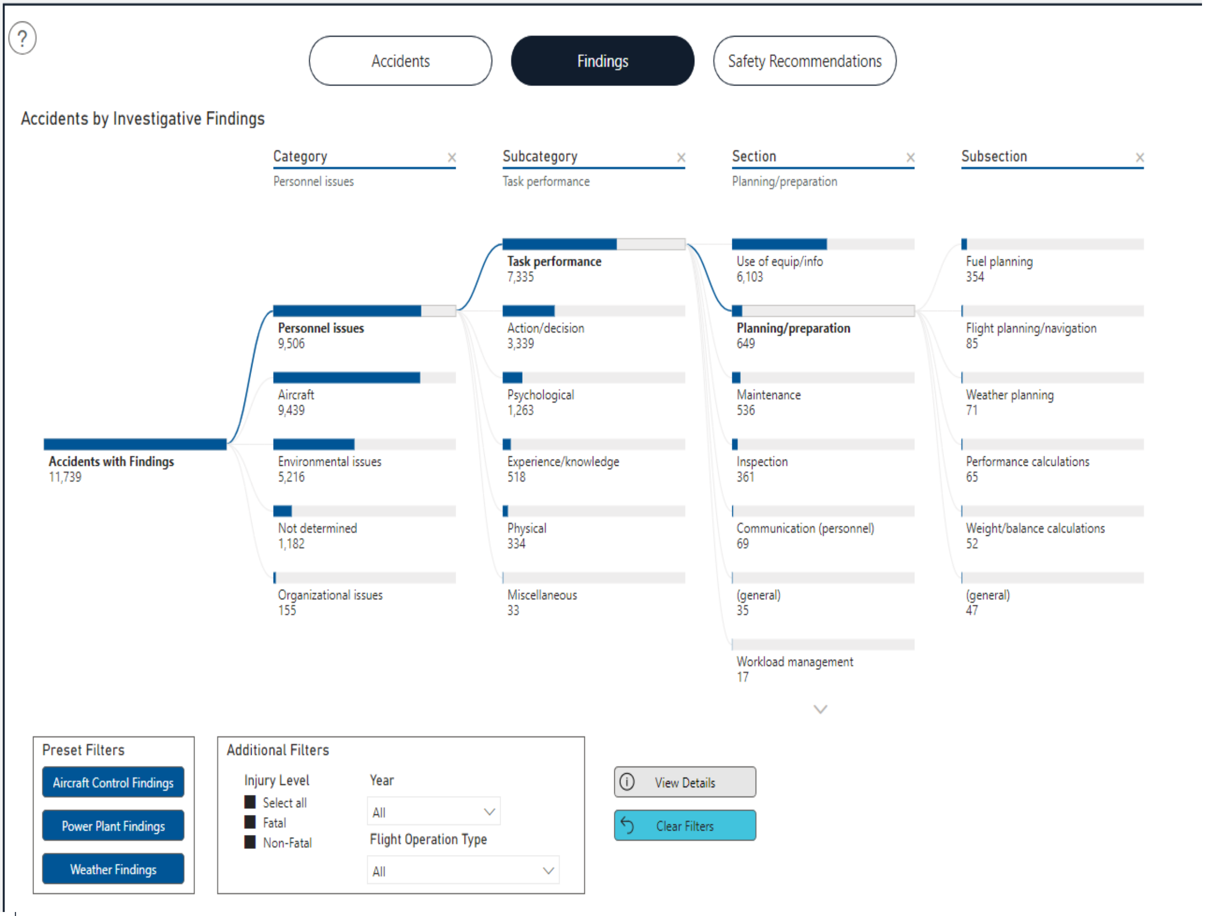
Summary Statistics

12,368	2,269	3,817
Accidents	Fatal Accidents	Fatalities

Filters

Flight Operation Type: All

State/Region: All



Category: Personnel issues

Subcategory: Task performance

Section: Planning/preparation

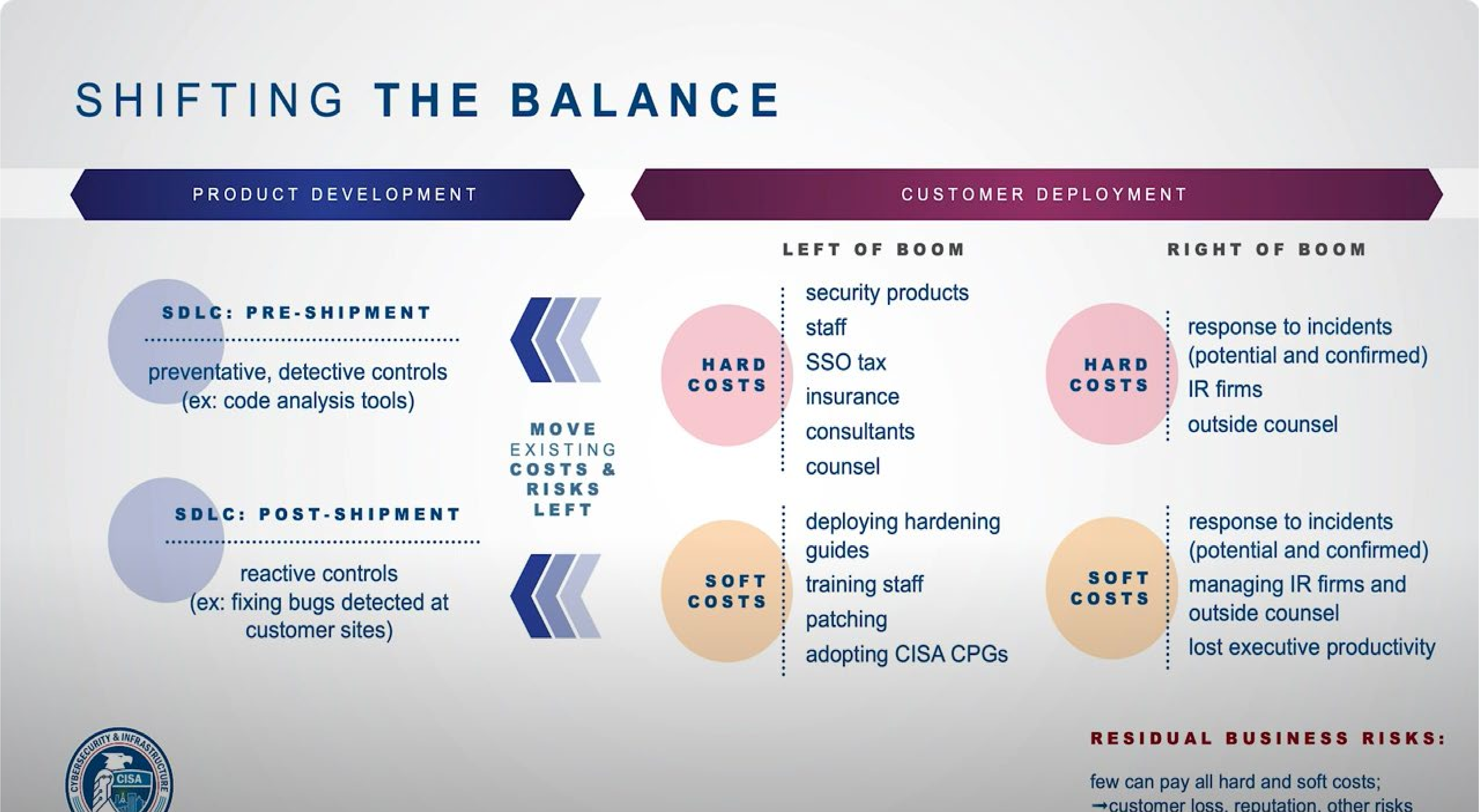
Subsection

Additional Filters

Injury Level
■ Select all
■ Fatal
■ Non-Fatal

Year: All

Flight Operation Type: All



SHIFTING THE BALANCE

PRODUCT DEVELOPMENT

SDLC: PRE-SHIPMENT

preventative, detective controls
(ex: code analysis tools)

SDLC: POST-SHIPMENT

reactive controls
(ex: fixing bugs detected at customer sites)

MOVE EXISTING **COSTS & RISKS LEFT**

CUSTOMER DEPLOYMENT

LEFT OF BOOM

HARD COSTS

- security products
- staff
- SSO tax
- insurance
- consultants
- counsel

SOFT COSTS

- deploying hardening guides
- training staff
- patching
- adopting CISA CPGs

RIGHT OF BOOM

HARD COSTS

- response to incidents (potential and confirmed)
- IR firms
- outside counsel

SOFT COSTS

- response to incidents (potential and confirmed)
- managing IR firms and outside counsel
- lost executive productivity

RESIDUAL BUSINESS RISKS:

few can pay all hard and soft costs;
➞customer loss, reputation, other risks

Unsafe At Any Speed: CISA's Plan to Foster Tech Ecosystem Security - YouTube

SECURE BY **DESIGN**

VS.

SECURE BY **DEFAULT**

SECURE BY **DESIGN**

1. is a business level goal
2. stated before design kick-off
3. requires real tradeoffs
4. can't be added later

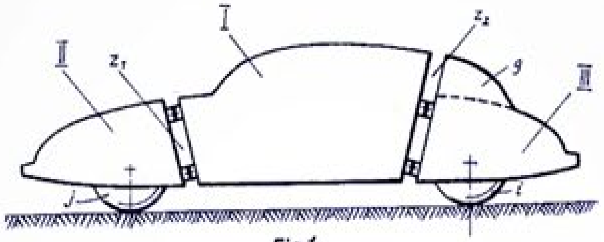
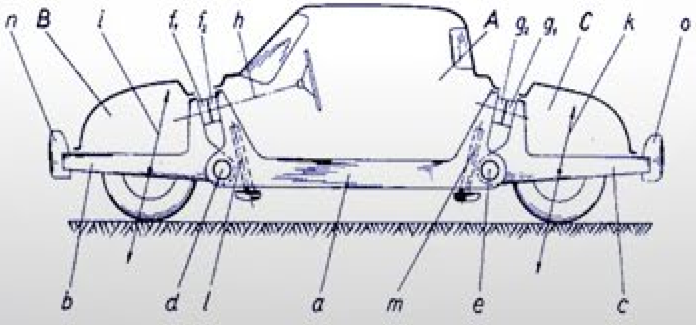
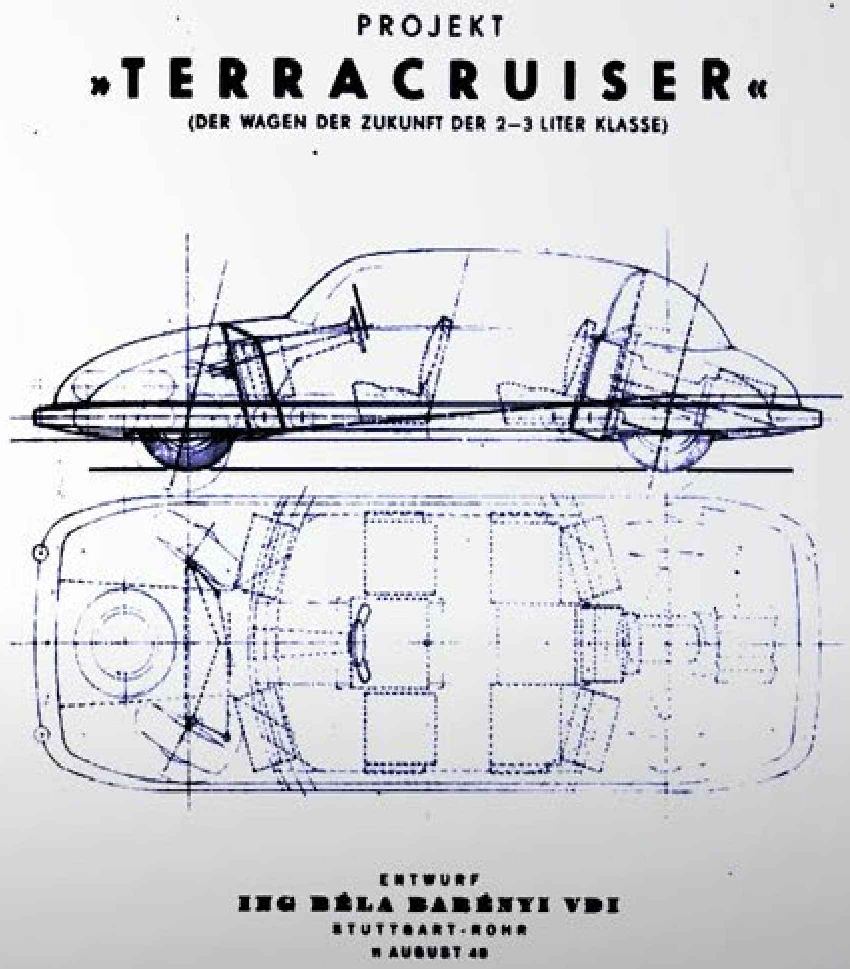
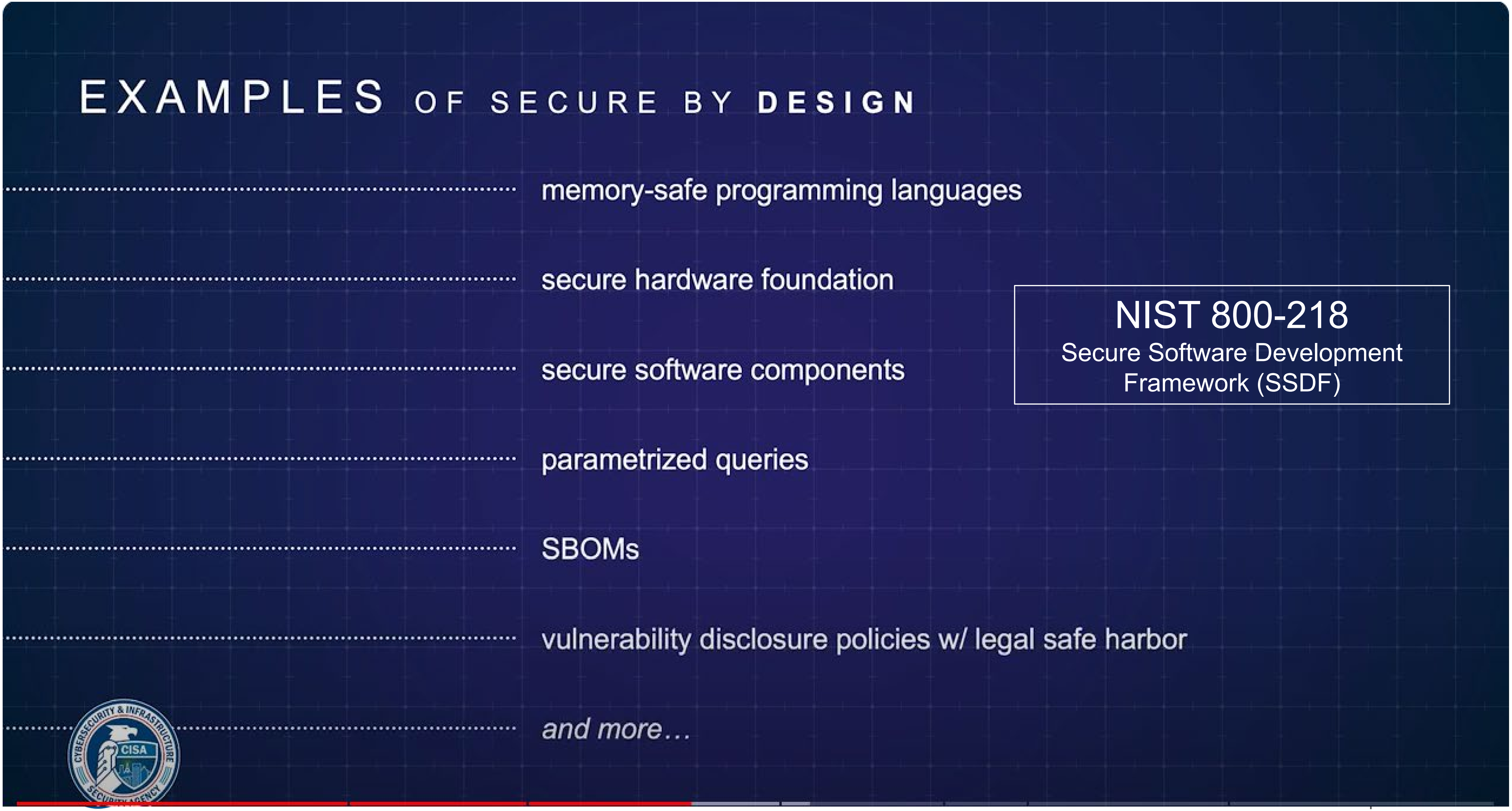


Fig.1.





Unsafe At Any Speed: CISA's Plan to Foster Tech Ecosystem Security - YouTube



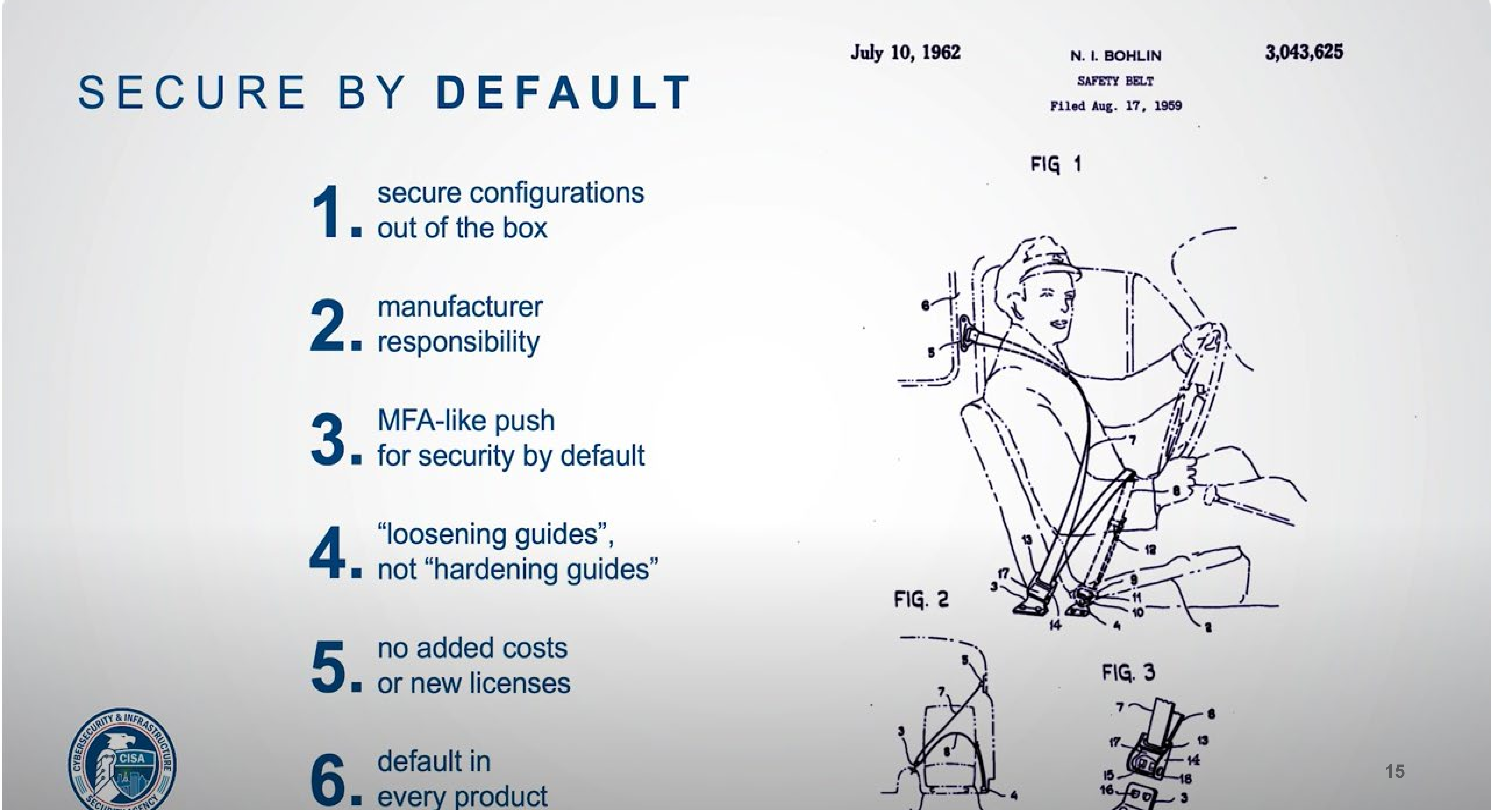
EXAMPLES OF SECURE BY DESIGN

- memory-safe programming languages
- secure hardware foundation
- secure software components
- parametrized queries
- SBOMs
- vulnerability disclosure policies w/ legal safe harbor
- *and more…*

NIST 800-218
Secure Software Development Framework (SSDF)

[Unsafe At Any Speed: CISA's Plan to Foster Tech Ecosystem Security - YouTube]

SECURE BY **DEFAULT**



SECURE BY DEFAULT

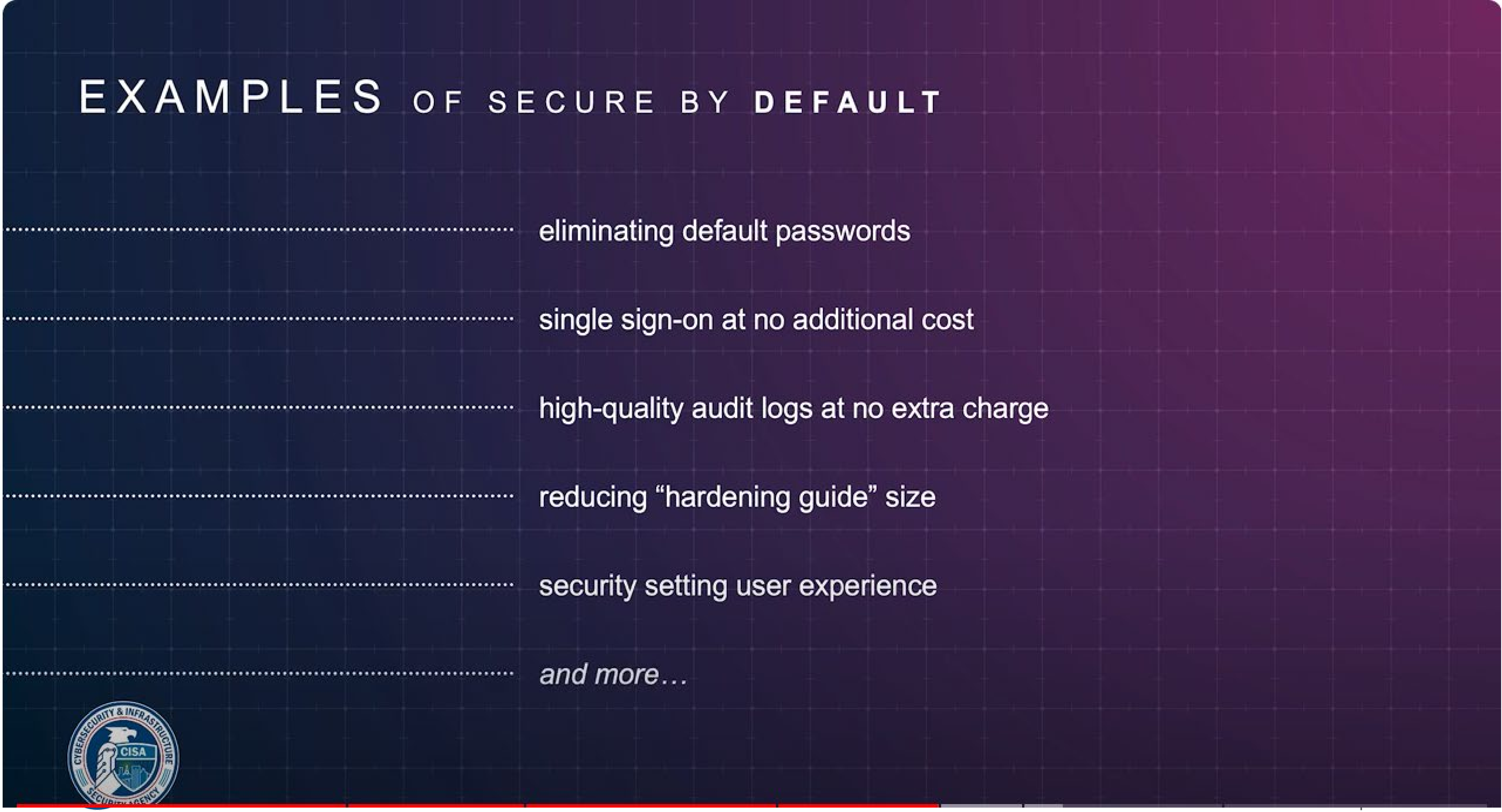
1. secure configurations out of the box
2. manufacturer responsibility
3. MFA-like push for security by default
4. “loosening guides”, not “hardening guides”
5. no added costs or new licenses
6. default in every product

July 10, 1962 N. I. BOHLIN 3,043,625

SAFETY BELT

Filed Aug. 17, 1959

Unsafe At Any Speed: CISA's Plan to Foster Tech Ecosystem Security - YouTube



EXAMPLES OF SECURE BY DEFAULT

- eliminating default passwords
- single sign-on at no additional cost
- high-quality audit logs at no extra charge
- reducing “hardening guide” size
- security setting user experience
- *and more…*

Unsafe At Any Speed: CISA's Plan to Foster Tech Ecosystem Security - YouTube

CYBER THREATS

Cyber Actors and Capabilities

	State Actors with Greater Capabilities	State Actors with Lesser Capabilities	Cybercriminals	Criminal Hackers	Terrorists
Damage to Critical Infrastructure	■	▨			
Disruption to Critical Infrastructure	■	■	■		
Theft of Intellectual Property/Financial Data	■	■	■	▨	▨
Theft of Sensitive Information (PII)	■	■	■	■	■
Establish and Maintain Illicit Presence	■	■	■	■	▨
Denial of Service (DoS)	■	■	■	■	■
Web Defacements	■	■	■	■	■

Source: I&A analysis derived from media and USG reporting

Note: Darker color indicates greater capability .

Cyber Threats of Today

Business Email Compromise

- 2 Billion in U.S. Loss FY-22
- Credential Stealing
- Phishing/ PopUps/ Poison Domains/ Onsite Exchange Vulnerabilities
- Steals Data
- Finance Diversions
- SupplyChain/External Dependencies Exploitation

Ransomware

- 34 Million in Loss FY-22
- 700K per Victim
- Lockbit, Royal, AvosLocker, Conti, Darkside, Maui
- Russian and North Korea State Actors
- Steals and Encrypts Data
- Double Extortion
- Destructive Malware Trends- Russia
  - Hermeticwiper and Wispergate

Common Defensive Measures

- Multifactor Authentication (MFA)
- Backups- Off Network
- Vulnerability Management – Patching
- Configuration Management - RDP, SMB, etc
- Log Management and Review

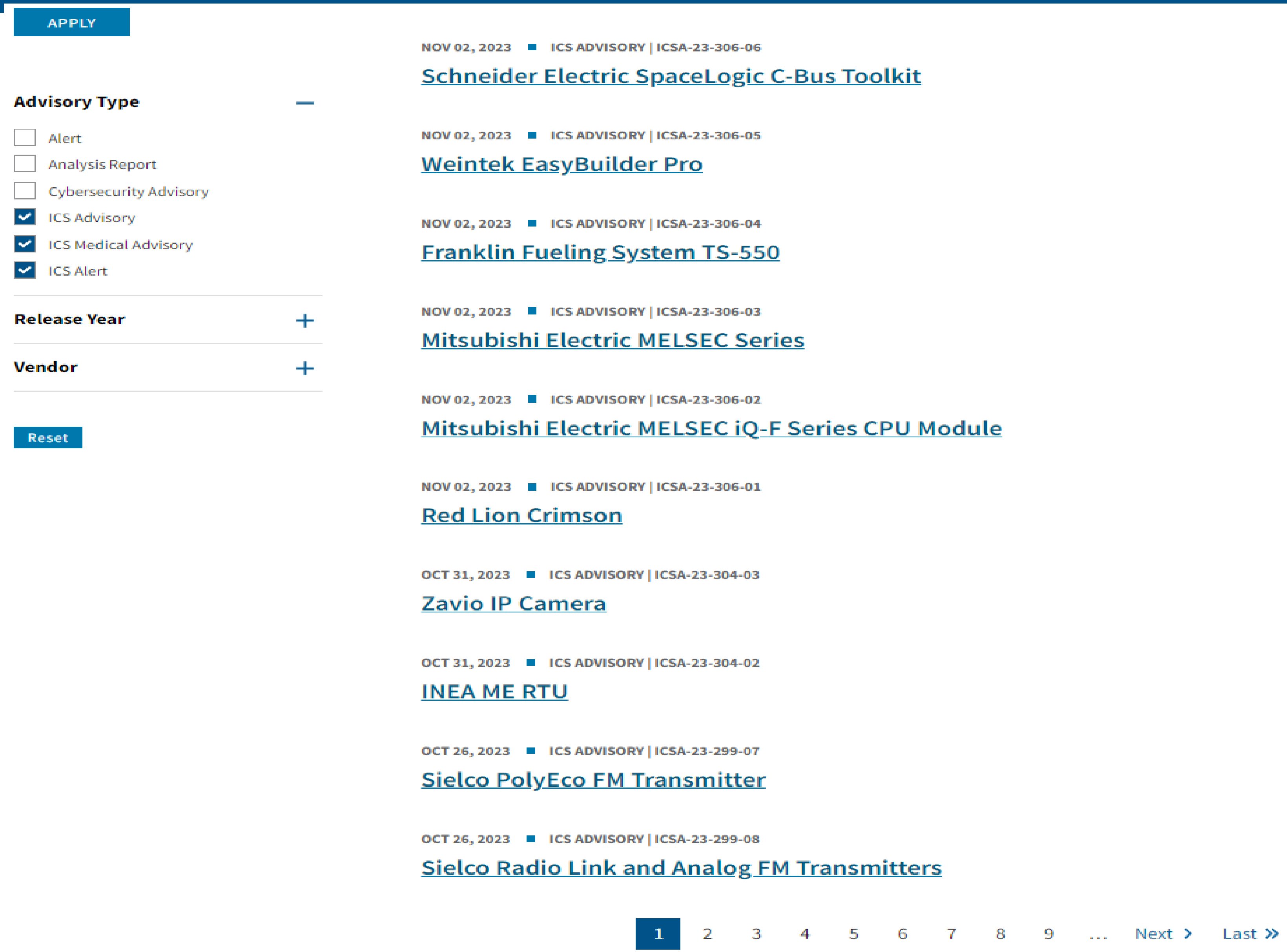
Volt Typhoon – Chinese State Actor

- Living-Off-The-Land Technique
- PowerShell, WMI, and CMD use
- Leverages scheduled tasks
- Use of domestic home users as C2
- Deleting Logs (event 1102)

Operational Technology (OT) Vulnerabilities

- Building Automation Systems (BAS) BACNet Field Panels (BFP)
  - HVAC Systems Control- elevators, lighting, emergency services, sensors, access control, etc.
- Diagnostic Systems - CT, Ultrasound, MRI, Imaging etc.
    - Picture Archiving Communication System (PACS) network
    - Digital Imaging and Communications in Medicine (DICOM) format
- Medical Devices – Infusion pumps, patient monitors
- Utility PLCs (programable logic controller)
- Camera Systems

Industrial Control Systems Advisories



APPLY

Advisory Type —

- ☐ Alert
- ☐ Analysis Report
- ☐ Cybersecurity Advisory
- ☑ ICS Advisory
- ☑ ICS Medical Advisory
- ☑ ICS Alert

Release Year +

Vendor +

Reset

NOV 02, 2023 ■ ICS ADVISORY | ICSA-23-306-06
Schneider Electric SpaceLogic C-Bus Toolkit

NOV 02, 2023 ■ ICS ADVISORY | ICSA-23-306-05
Weintek EasyBuilder Pro

NOV 02, 2023 ■ ICS ADVISORY | ICSA-23-306-04
Franklin Fueling System TS-550

NOV 02, 2023 ■ ICS ADVISORY | ICSA-23-306-03
Mitsubishi Electric MELSEC Series

NOV 02, 2023 ■ ICS ADVISORY | ICSA-23-306-02
Mitsubishi Electric MELSEC iQ-F Series CPU Module

NOV 02, 2023 ■ ICS ADVISORY | ICSA-23-306-01
Red Lion Crimson

OCT 31, 2023 ■ ICS ADVISORY | ICSA-23-304-03
Zavio IP Camera

OCT 31, 2023 ■ ICS ADVISORY | ICSA-23-304-02
INEA ME RTU

OCT 26, 2023 ■ ICS ADVISORY | ICSA-23-299-07
Sielco PolyEco FM Transmitter

OCT 26, 2023 ■ ICS ADVISORY | ICSA-23-299-08
Sielco Radio Link and Analog FM Transmitters

CISA ICS No-Cost Virtual Training

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour

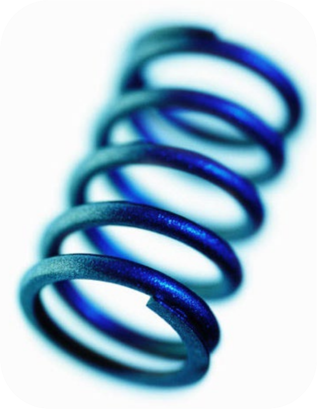
https://www.cisa.gov/ics-training-available-through-cisa

CISA CYBERSECURITY SERVICES

Resilience Defined

"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

- Presidential Policy Directive 21
February 12, 2013



Protect (Security)	**Sustain (Continuity)**
Perform (Capability)	**Repeat (Maturity)**

Cybersecurity Advisor Program (CSA)

Partnership Development

- Outreach Activities
- Informational Exchanges (individual, group, etc.)
- Committees and Working Groups support
- Symposiums/ Conferences/ Webinars/ Cyber Camps
- FBI Cyber Task Force Memberships

Stakeholder Preparedness

- Cybersecurity Workshops
- Technical Exchange
- Introductory Visits and Cyber Protective Visits (CPVs)
- Cyber Exercises support/ *Tabletop Exercises*
- Awareness and Cyber Threat Training/ Briefings

Assessments

- Cybersecurity Performance Goals assessments (CPGs)
- Ransomware Readiness Assessments (RRAs)
- Cyber Resilience Reviews (CRRs)
- External Dependency Management Assessments (EDMs)

Vulnerability Scanning

- Cyber Hygiene Service (Public Attack Surface)
  - Known Exploitable Vulnerabilities (KEV)
- Web Application Scanning
- Penetration Testing

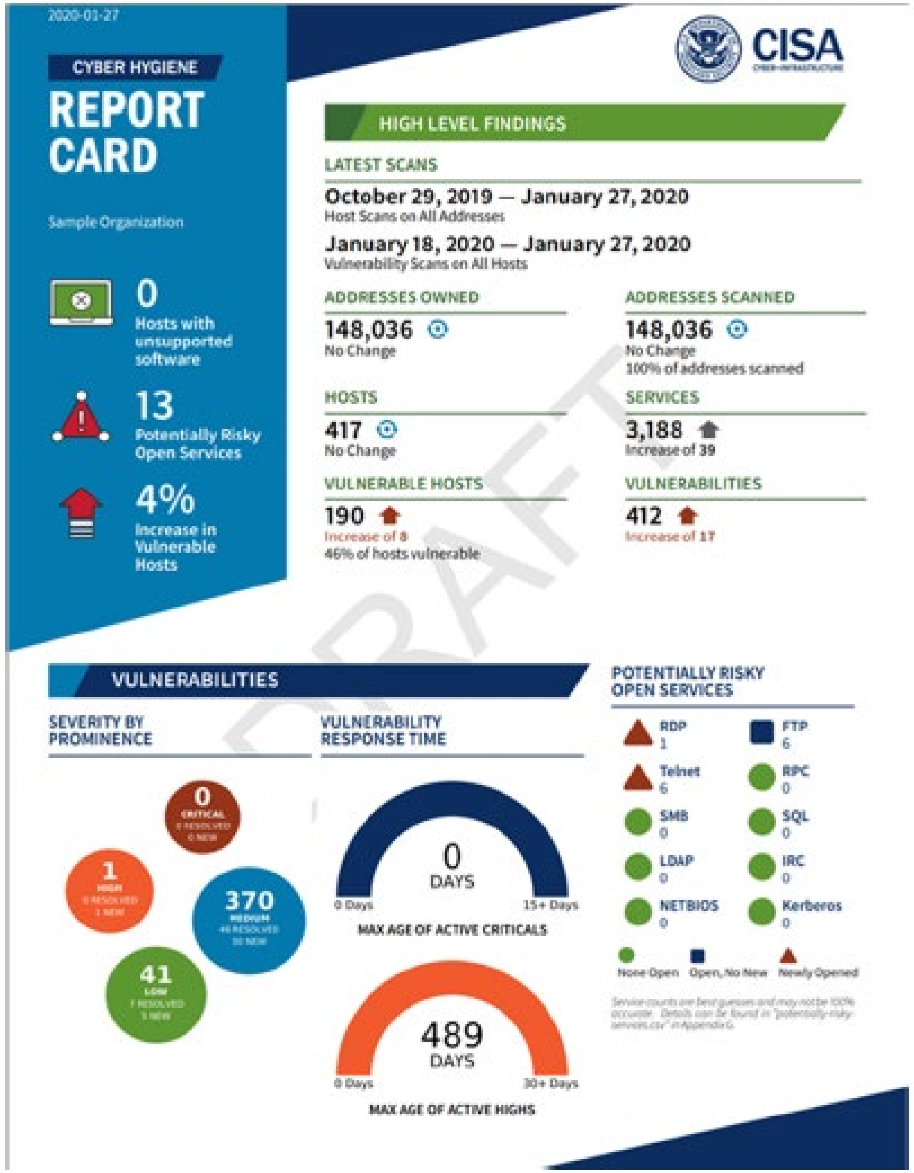
Cyber Hygiene Report Card

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services



2020-01-27

CYBER HYGIENE

REPORT CARD

Sample Organization

0 Hosts with unsupported software

13 Potentially Risky Open Services

4% Increase in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

October 29, 2019 — January 27, 2020
Host Scans on All Addresses

January 18, 2020 — January 27, 2020
Vulnerability Scans on All Hosts

ADDRESSES OWNED
148,036
No Change

ADDRESSES SCANNED
148,036
No Change
100% of addresses scanned

HOSTS
417
No Change

SERVICES
3,188
Increase of 39

VULNERABLE HOSTS
190
Increase of 8
46% of hosts vulnerable

VULNERABILITIES
412
Increase of 17

VULNERABILITIES

SEVERITY BY PROMINENCE

0 CRITICAL 0 RESOLVED 0 NEW

1 HIGH 0 RESOLVED 1 NEW

370 MEDIUM 46 RESOLVED 30 NEW

41 LOW 7 RESOLVED 5 NEW

VULNERABILITY RESPONSE TIME

0 DAYS (0 Days – 15+ Days)
MAX AGE OF ACTIVE CRITICALS

489 DAYS (0 Days – 30+ Days)
MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

▲	RDP 1	■	FTP 6
▲	Telnet 6	●	RPC 0
●	SMB 0	●	SQL 0
●	LDAP 0	●	IRC 0
●	NETBIOS 0	●	Kerberos 0

● None Open ■ Open, No New ▲ Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

CISA No-Cost Cybersecurity Tools

Assess Vulnerabilities:

- Downloading and Installing CSET | CISA
- Known Exploited Vulnerabilities Catalog | CISA

Hardening:

- CIS Benchmarks (cisecurity.org)
- GitHub - decalage2/awesome-security-hardening: A collection of awesome security hardening guides, tools and other resources
- Secure Cloud Business Applications (SCuBA) Project | CISA
  - GitHub - cisagov/ScubaGear: Automation to assess the state of your M365 tenant against CISA's baselines
  - https://www.cisa.gov/sites/default/files/publications/SCuBA_TRA_RFC_EG_508c.pdf

Cyber Defense:

- Helping Cyber Defenders "Decide" to Use MITRE ATT&CK | CISA
- Logging Made Easy SIEM Tool
- CISA Releases RedEye: Red Team Campaign Visualization and Reporting Tool | CISA
- CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks | CISA
- Cyber Career Pathways Tool | CISA

Report and Incident and Software Vulnerability

- CISA: **cisa.gov/report** ; report@cisa.gov, (888) 282-0870
- FBI/ Internet Crime Complaint Center (IC3): **ic3.gov**

Resources: CISA.GOV

Contact Information

Joe Parker
Region 4 Cybersecurity Advisor – Huntsville, AL
Joseph.Parker@cisa.dhs.gov
(202) 894-4869 (Cell)

Stephanie Watt
Alabama Cybersecurity State Coordinator/ Advisor – Montgomery, AL
Stephanie.Watt@cisa.dhs.gov
(202) 615-4615 (Cell)

Clyde Roark
Region 4 Cybersecurity Advisor - Mobile, AL
Clyde.Roark@cisa.dhs.gov
(850) 776-2894 (Cell)