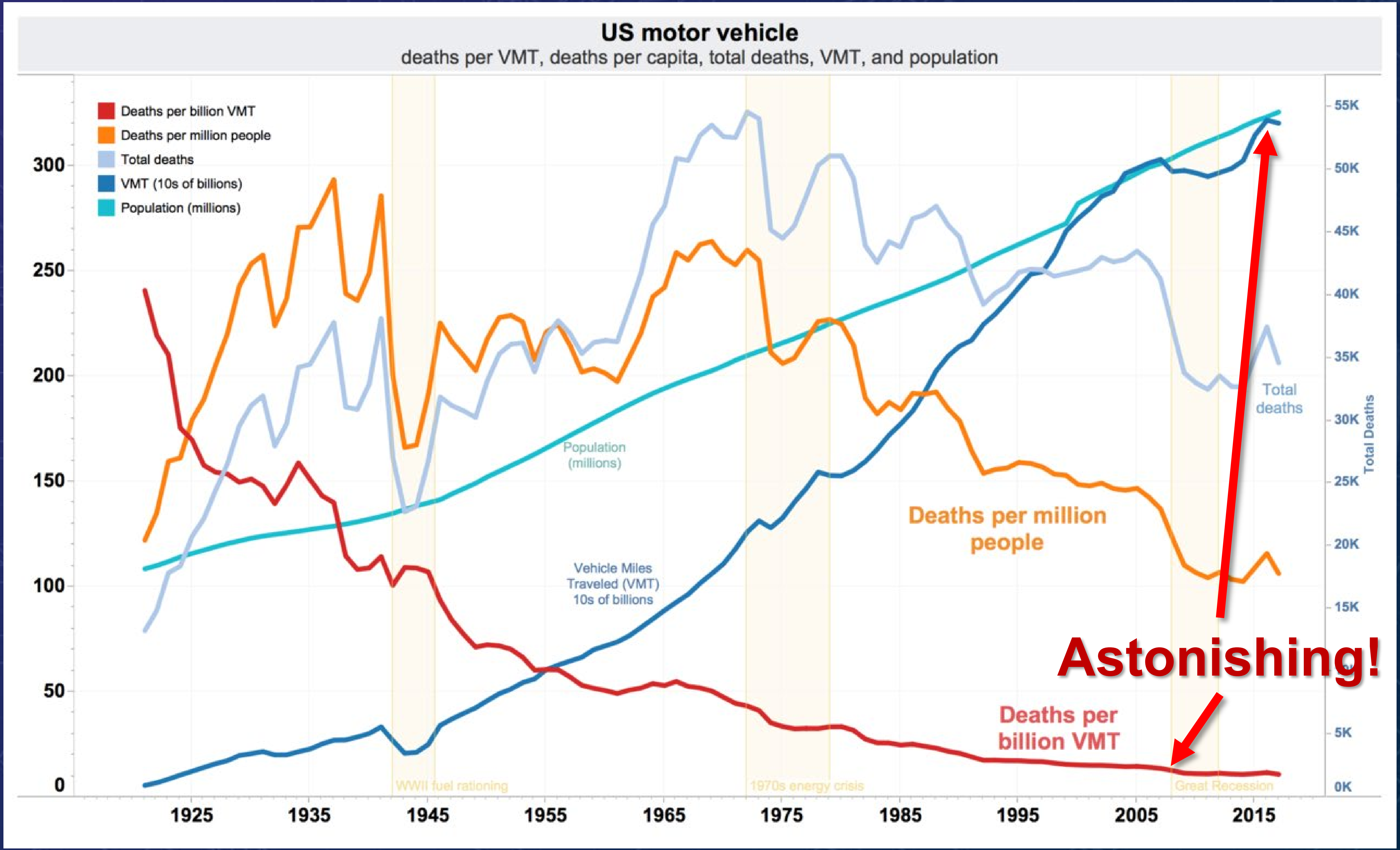
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

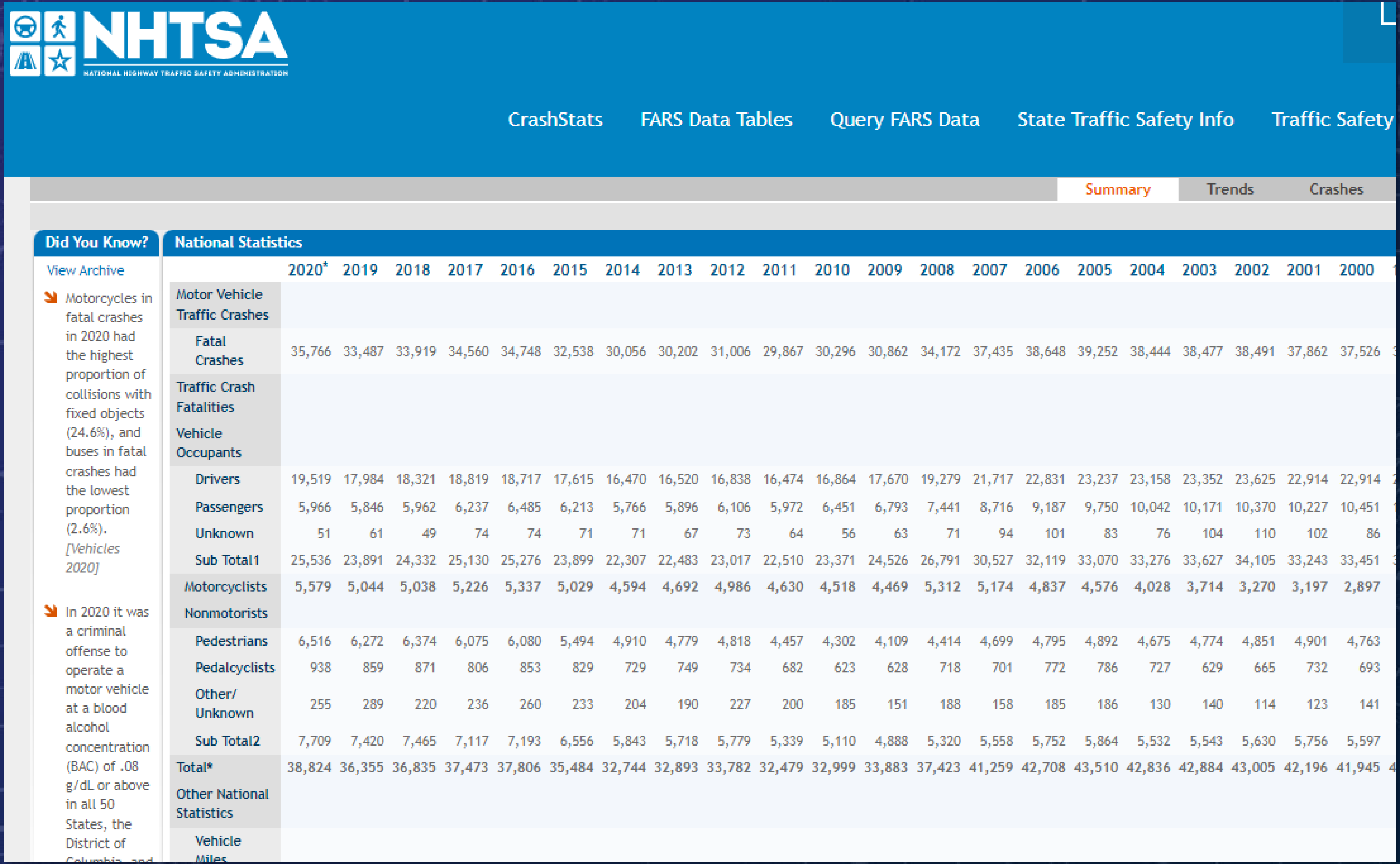
SECURE BY DESIGN

WHAT DO MATURE INDUSTRIES LOOK LIKE?



Astonishing!

FATALITY ANALYSIS REPORTING SYSTEM (FARS)



Did You Know?

View Archive

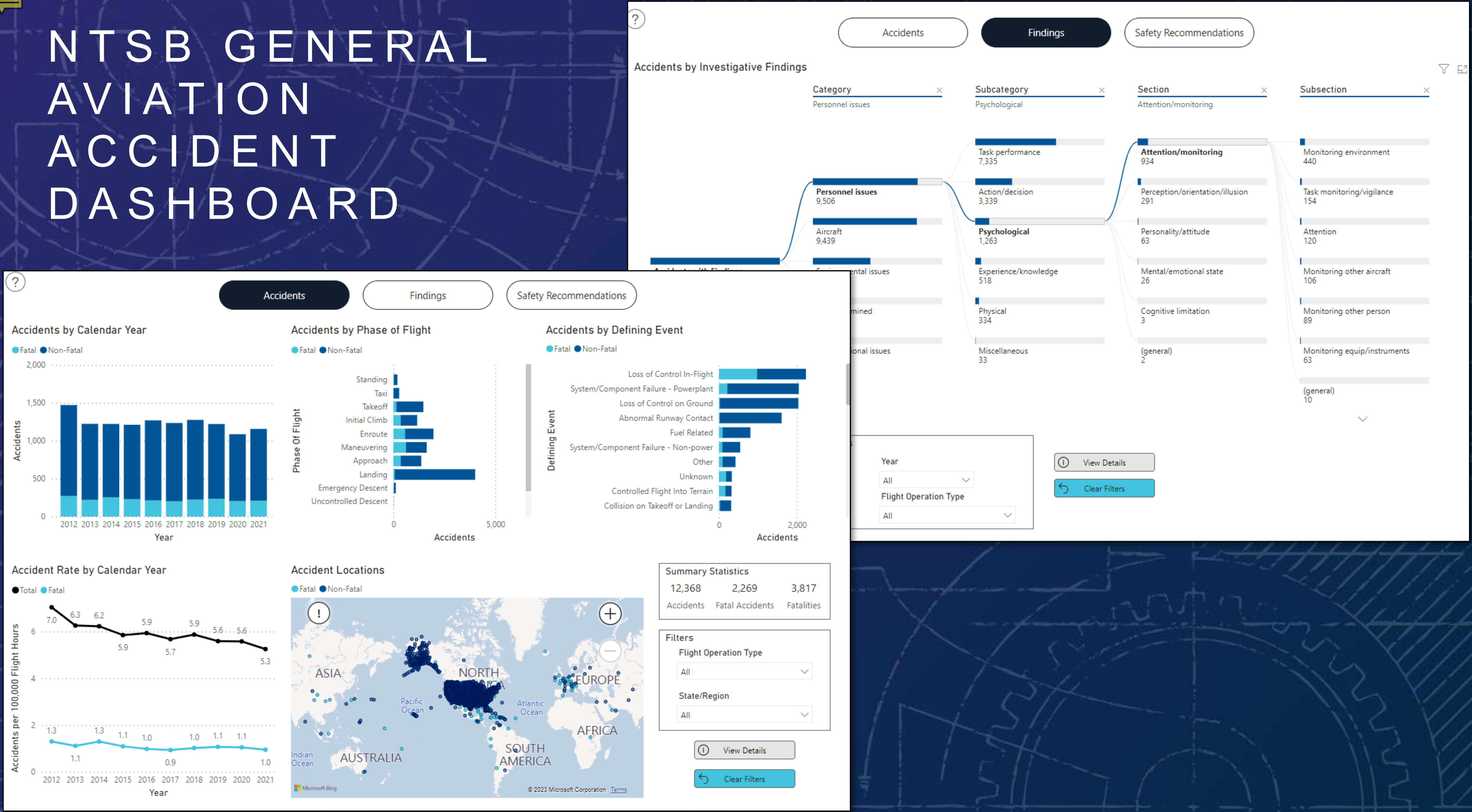
Motorcycles in fatal crashes in 2020 had the highest proportion of collisions with fixed objects (24.6%), and buses in fatal crashes had the lowest proportion (2.6%). *[Vehicles 2020]*

In 2020 it was a criminal offense to operate a motor vehicle at a blood alcohol concentration (BAC) of .08 g/dL or above in all 50 States, the District of Columbia, and

National Statistics

	2020*	2019	2018	2017	2016	2015	2014	2013	2012	2011	2010	2009	2008	2007	2006	2005	2004	2003	2002	2001	2000
Motor Vehicle Traffic Crashes																					
Fatal Crashes	35,766	33,487	33,919	34,560	34,748	32,538	30,056	30,202	31,006	29,867	30,296	30,862	34,172	37,435	38,648	39,252	38,444	38,477	38,491	37,862	37,526
Traffic Crash Fatalities																					
Vehicle Occupants																					
Drivers	19,519	17,984	18,321	18,819	18,717	17,615	16,470	16,520	16,838	16,474	16,864	17,670	19,279	21,717	22,831	23,237	23,158	23,352	23,625	22,914	22,914
Passengers	5,966	5,846	5,962	6,237	6,485	6,213	5,766	5,896	6,106	5,972	6,451	6,793	7,441	8,716	9,187	9,750	10,042	10,171	10,370	10,227	10,451
Unknown	51	61	49	74	74	71	71	67	73	64	56	63	71	94	101	83	76	104	110	102	86
Sub Total1	25,536	23,891	24,332	25,130	25,276	23,899	22,307	22,483	23,017	22,510	23,371	24,526	26,791	30,527	32,119	33,070	33,276	33,627	34,105	33,243	33,451
Motorcyclists	5,579	5,044	5,038	5,226	5,337	5,029	4,594	4,692	4,986	4,630	4,518	4,469	5,312	5,174	4,837	4,576	4,028	3,714	3,270	3,197	2,897
Nonmotorists																					
Pedestrians	6,516	6,272	6,374	6,075	6,080	5,494	4,910	4,779	4,818	4,457	4,302	4,109	4,414	4,699	4,795	4,892	4,675	4,774	4,851	4,901	4,763
Pedalcyclists	938	859	871	806	853	829	729	749	734	682	623	628	718	701	772	786	727	629	665	732	693
Other/ Unknown	255	289	220	236	260	233	204	190	227	200	185	151	188	158	185	186	130	140	114	123	141
Sub Total2	7,709	7,420	7,465	7,117	7,193	6,556	5,843	5,718	5,779	5,339	5,110	4,888	5,320	5,558	5,752	5,864	5,532	5,543	5,630	5,756	5,597
Total*	38,824	36,355	36,835	37,473	37,806	35,484	32,744	32,893	33,782	32,479	32,999	33,883	37,423	41,259	42,708	43,510	42,836	42,884	43,005	42,196	41,945
Other National Statistics																					
Vehicle Miles																					

NTSB GENERAL AVIATION ACCIDENT DASHBOARD



Year: All

Flight Operation Type: All

Summary Statistics

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

Filters

Flight Operation Type: All

State/Region: All

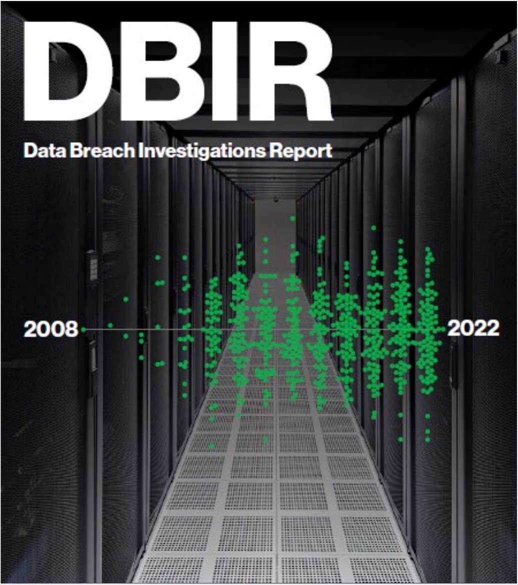
HOW DOES THE SOFTWARE INDUSTRY COMPARE?

SOURCES OF INFO

Microsoft

Microsoft Digital Defense Report 2022

Illuminating the threat landscape and empowering a digital defense.



DBIR

Data Breach Investigations Report

M-TRENDS 2022

MANDIANT SPECIAL REPORT

CROWDSTRIKE

2022 Global Threat

Many data sources

How do they help?

- Customers
- Manufacturers

BACKGROUND

April 13, 2023

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

Publication: April 13, 2023

Cybersecurity and Infrastructure Security Agency

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

Disclaimer: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when informa carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and Subject to standard copyright rules, TLP:CLEAR information may be distributed with the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

CISA // FBI // NSA // Australian Cyber Security Centre // Canadian Centre for Cyber Security // The National Cyber Security Center, UK // Federal Office for Information Security BSI, Germany // The National Cyber Security Centre, Netherlands // CERT NZ, New Zealand // National Cyber Security Centre, New Zealand

THE PROBLEM

SECURITY PRODUCTS

LOGS

PATCHES

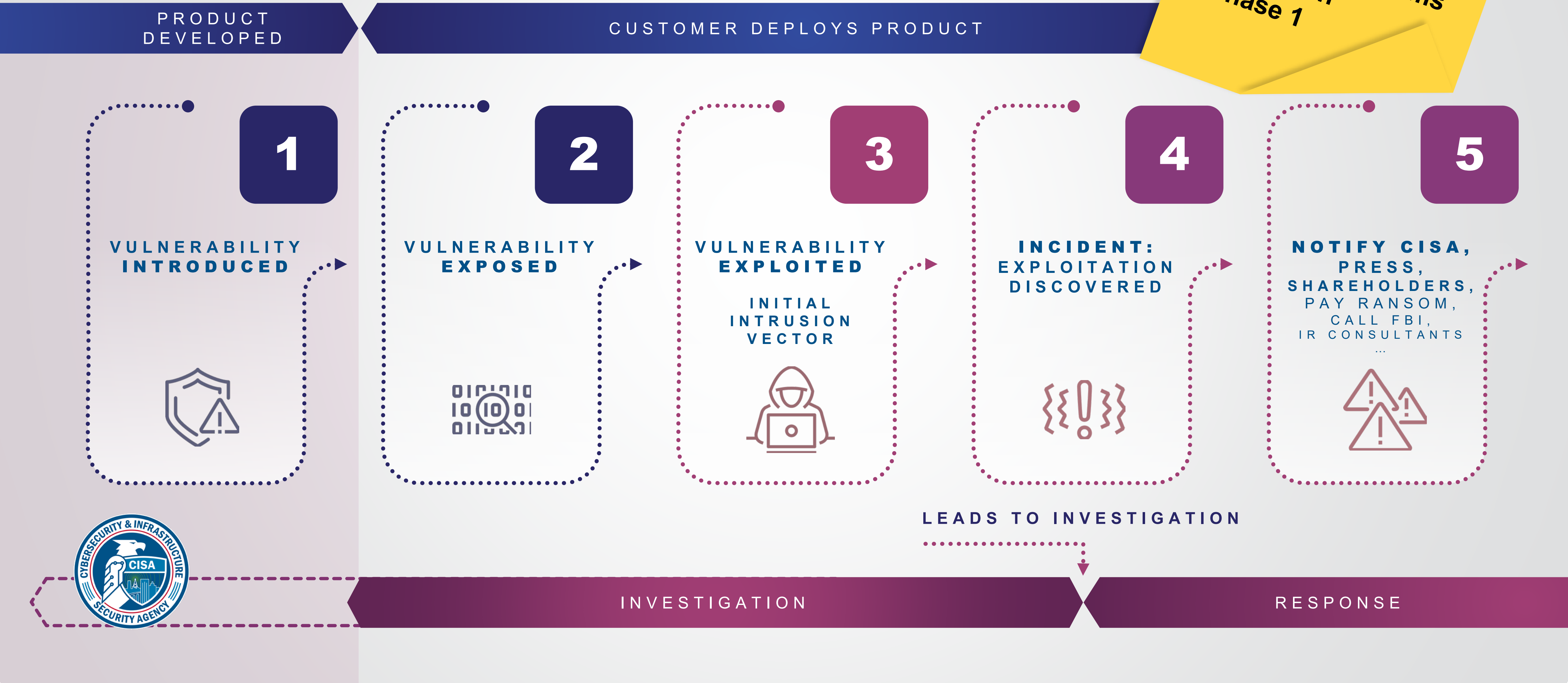
IAM

GUIDES

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

FROM CUSTOMER TO PRODUCT
LIFECYCLE INVESTIGATION

no amount of time and money spent in Phase 5 will stop the problems caused in Phase 1



PRODUCT DEVELOPED

CUSTOMER DEPLOYS PRODUCT

1 VULNERABILITY INTRODUCED

2 VULNERABILITY EXPOSED

3 VULNERABILITY EXPLOITED

INITIAL INTRUSION VECTOR

4 INCIDENT: EXPLOITATION DISCOVERED

5 NOTIFY CISA, PRESS, SHAREHOLDERS, PAY RANSOM, CALL FBI, IR CONSULTANTS …

LEADS TO INVESTIGATION

INVESTIGATION

RESPONSE

UNDERLYING PRINCIPLES

1. own security outcomes

2. transparency and accountability

3. organization structure

SECURE BY **DESIGN**

vs.

SECURE BY **DEFAULT**

SECURE BY **DESIGN**

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

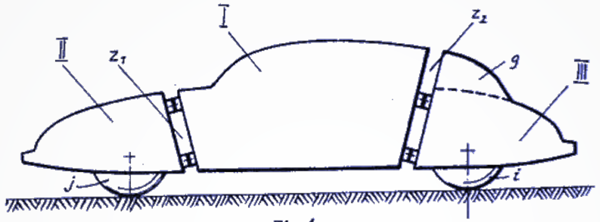
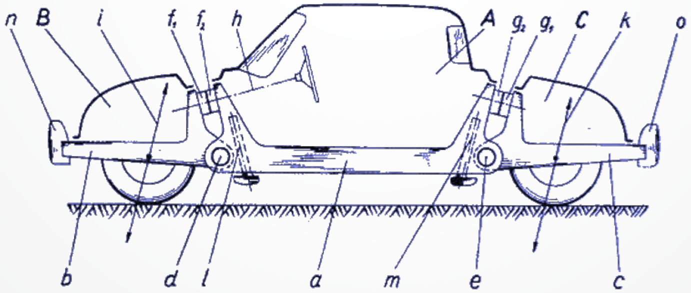
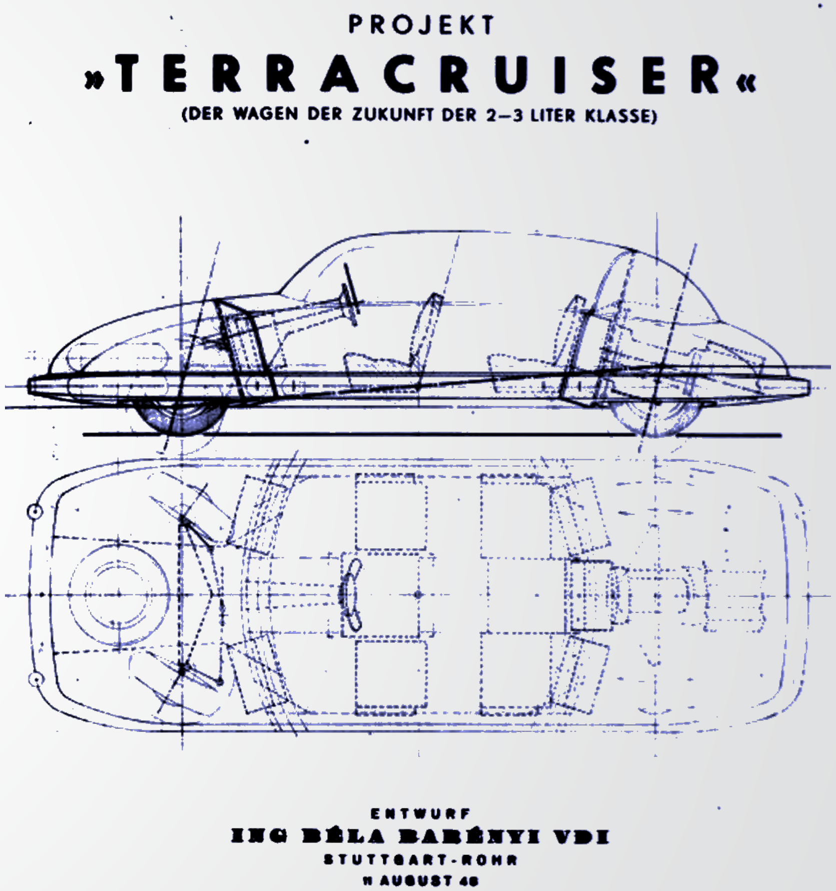
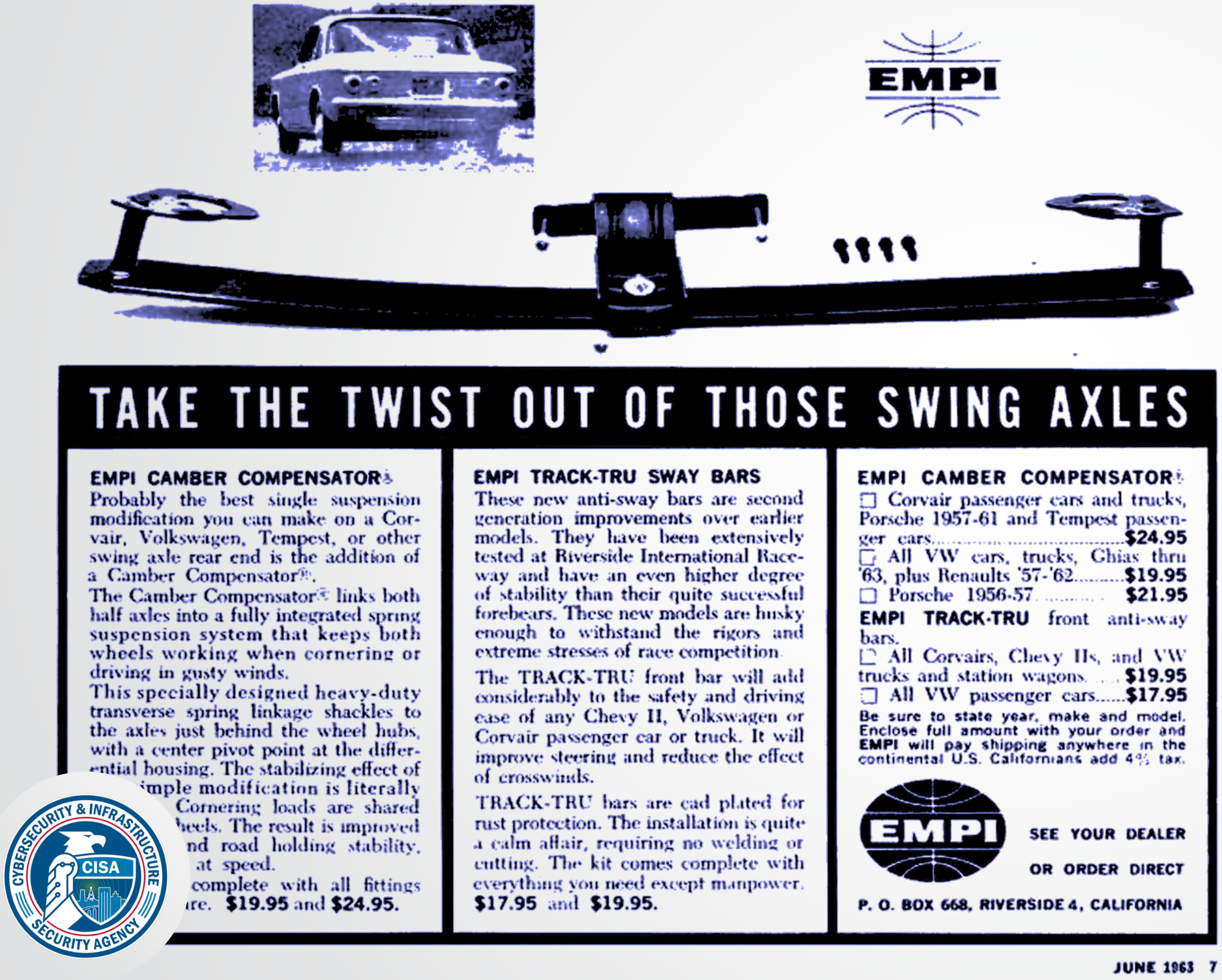


Fig.1.





COSTS OF LACK OF SAFETY BY DESIGN



TAKE THE TWIST OUT OF THOSE SWING AXLES

EMPI CAMBER COMPENSATOR®

Probably the best single suspension modification you can make on a Corvair, Volkswagen, Tempest, or other swing axle rear end is the addition of a Camber Compensator®.

The Camber Compensator® links both half axles into a fully integrated spring suspension system that keeps both wheels working when cornering or driving in gusty winds.

This specially designed heavy-duty transverse spring linkage shackles to the axles just behind the wheel hubs, with a center pivot point at the differential housing. The stabilizing effect of imple modification is literally Cornering loads are shared heels. The result is improved nd road holding stability, at speed.

complete with all fittings ire. **$19.95** and **$24.95.**

EMPI TRACK-TRU SWAY BARS

These new anti-sway bars are second generation improvements over earlier models. They have been extensively tested at Riverside International Raceway and have an even higher degree of stability than their quite successful forebears. These new models are husky enough to withstand the rigors and extreme stresses of race competition.

The TRACK-TRU front bar will add considerably to the safety and driving ease of any Chevy II, Volkswagen or Corvair passenger car or truck. It will improve steering and reduce the effect of crosswinds.

TRACK-TRU bars are cad plated for rust protection. The installation is quite a calm affair, requiring no welding or cutting. The kit comes complete with everything you need except manpower. **$17.95** and **$19.95.**

EMPI CAMBER COMPENSATOR®

□ Corvair passenger cars and trucks, Porsche 1957-61 and Tempest passenger cars.......... **$24.95**

□ All VW cars, trucks, Ghias thru '63, plus Renaults '57-'62.......... **$19.95**

□ Porsche 1956-57.......... **$21.95**

EMPI TRACK-TRU front anti-sway bars.

□ All Corvairs, Chevy IIs, and VW trucks and station wagons.......... **$19.95**

□ All VW passenger cars.......... **$17.95**

Be sure to state year, make and model. Enclose full amount with your order and EMPI will pay shipping anywhere in the continental U.S. Californians add 4% tax.

EMPI

SEE YOUR DEALER

OR ORDER DIRECT

P. O. BOX 668, RIVERSIDE 4, CALIFORNIA

JUNE 1963 7

> *"…keeps both wheels working when cornering or driving in gusty winds"*

> *"The result is improved handling and road holding stability, particularly at speed"*

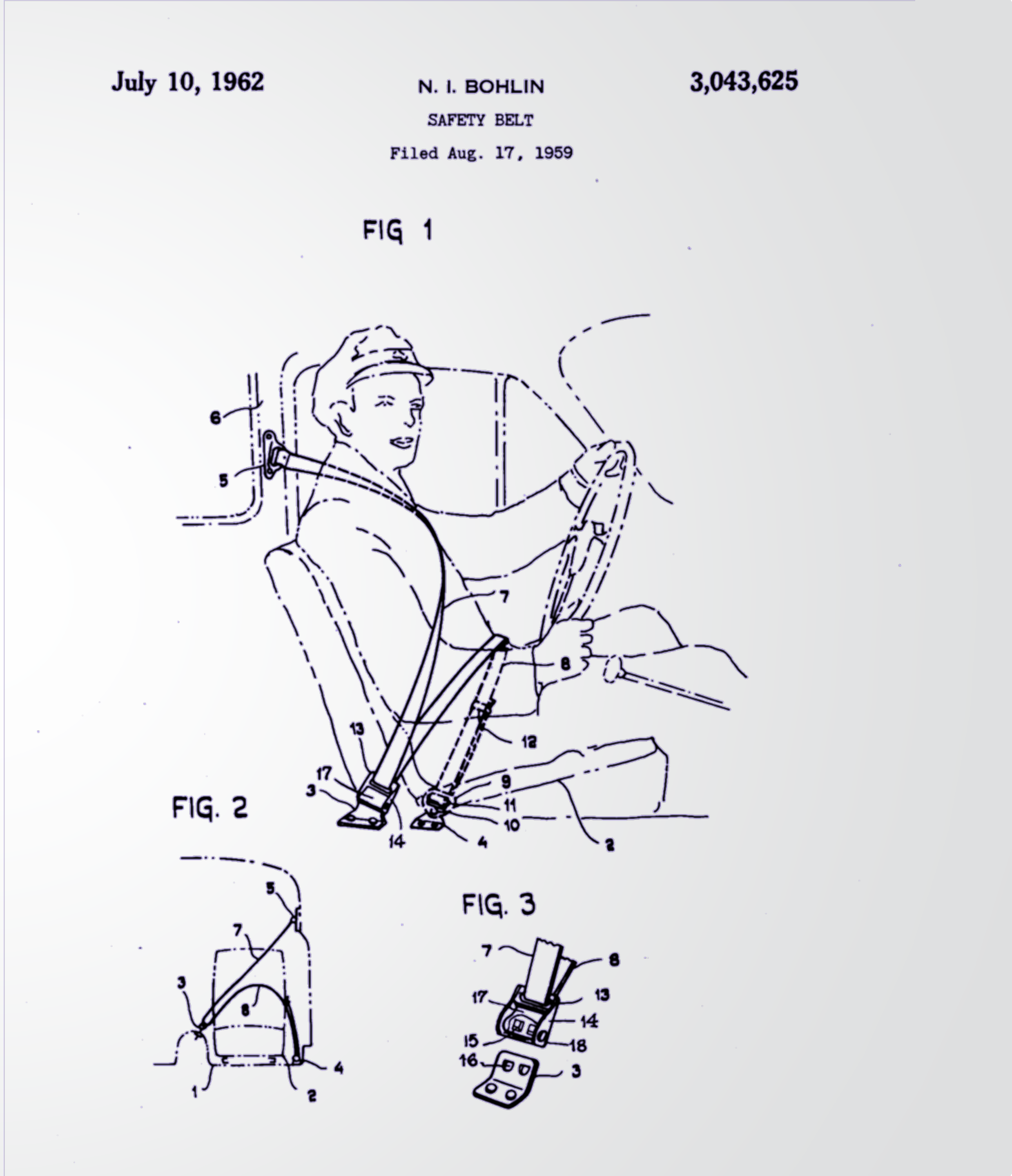
EXAMPLES OF SECURE BY **DESIGN**

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

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

FIG 1

FIG. 2

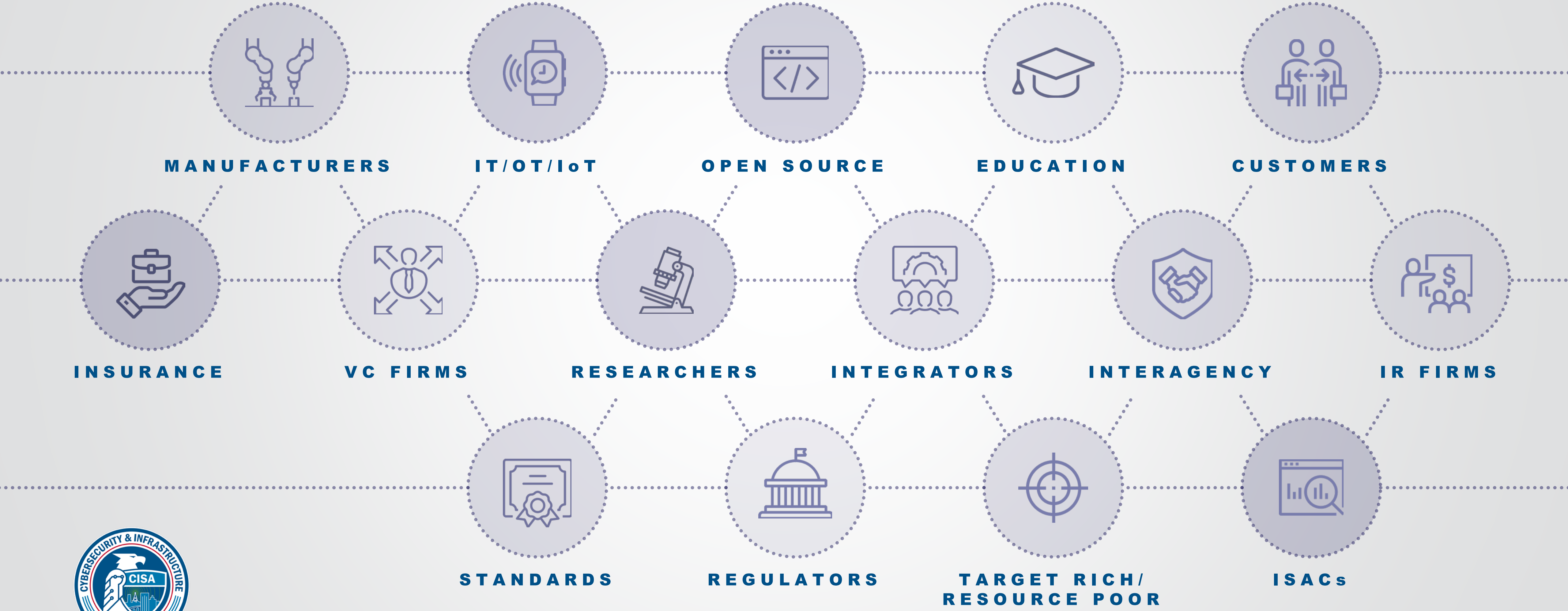
FIG. 3

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…*

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

SECURE BY DESIGN ECOSYSTEM



MANUFACTURERS

IT/OT/IoT

OPEN SOURCE

EDUCATION

CUSTOMERS

INSURANCE

VC FIRMS

RESEARCHERS

INTEGRATORS

INTERAGENCY

IR FIRMS

STANDARDS

REGULATORS

TARGET RICH/
RESOURCE POOR

ISACs

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

NATIONAL SECURITY DELTA:

the sum of individual risks creates an even larger national security risk though supply chain and other connections

BOTTOM LINE:

customers already pay a silent security tax; we want to shift that poorly measured and unevenly distributed tax to the left, reducing the overall costs and risks to customers

RESIDUAL BUSINESS RISKS:

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

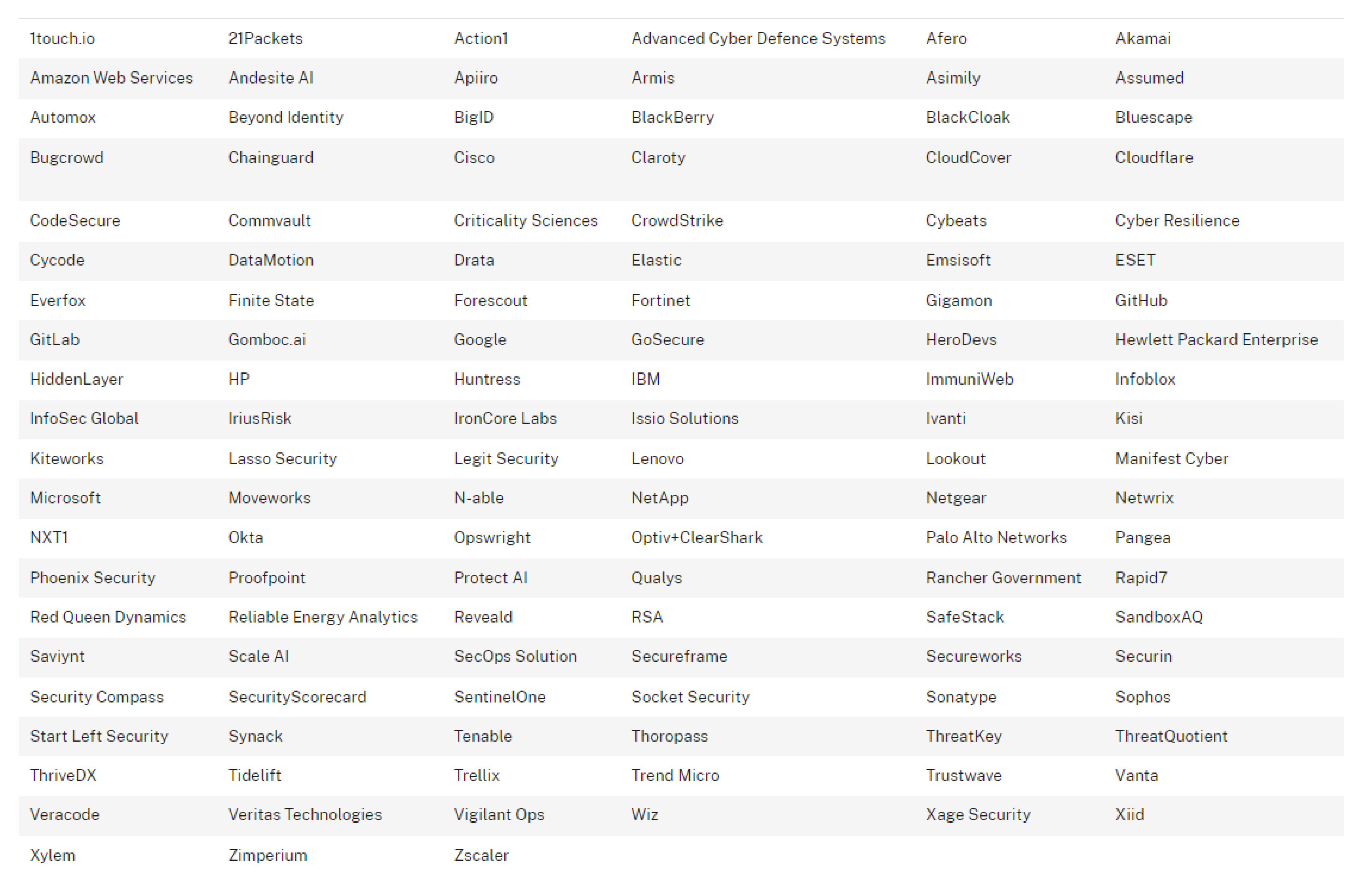
What can manufacturers do?

SECURE BY DESIGN
PLEDGE

Within a year, demonstrate measurable progress in the following areas:

1. Increase the use of multi-factor authentication (MFA).
2. Reduce default passwords across products.
3. Reduce entire classes of vulnerabilities.
4. Increase the installation of security patches by customers.
5. Publish a vulnerability disclosure policy (VDP).
6. Transparency in vulnerability reporting.
7. Increase in the ability for customers to gather evidence of intrusions.

SECURE BY DESIGN PLEDGE



1touch.io	21Packets	Action1	Advanced Cyber Defence Systems	Afero	Akamai
Amazon Web Services	Andesite AI	Apiiro	Armis	Asimily	Assumed
Automox	Beyond Identity	BigID	BlackBerry	BlackCloak	Bluescape
Bugcrowd	Chainguard	Cisco	Claroty	CloudCover	Cloudflare
CodeSecure	Commvault	Criticality Sciences	CrowdStrike	Cybeats	Cyber Resilience
Cycode	DataMotion	Drata	Elastic	Emsisoft	ESET
Everfox	Finite State	Forescout	Fortinet	Gigamon	GitHub
GitLab	Gomboc.ai	Google	GoSecure	HeroDevs	Hewlett Packard Enterprise
HiddenLayer	HP	Huntress	IBM	ImmuniWeb	Infoblox
InfoSec Global	IriusRisk	IronCore Labs	Issio Solutions	Ivanti	Kisi
Kiteworks	Lasso Security	Legit Security	Lenovo	Lookout	Manifest Cyber
Microsoft	Moveworks	N-able	NetApp	Netgear	Netwrix
NXT1	Okta	Opswright	Optiv+ClearShark	Palo Alto Networks	Pangea
Phoenix Security	Proofpoint	Protect AI	Qualys	Rancher Government	Rapid7
Red Queen Dynamics	Reliable Energy Analytics	Reveald	RSA	SafeStack	SandboxAQ
Saviynt	Scale AI	SecOps Solution	Secureframe	Secureworks	Securin
Security Compass	SecurityScorecard	SentinelOne	Socket Security	Sonatype	Sophos
Start Left Security	Synack	Tenable	Thoropass	ThreatKey	ThreatQuotient
ThriveDX	Tidelift	Trellix	Trend Micro	Trustwave	Vanta
Veracode	Veritas Technologies	Vigilant Ops	Wiz	Xage Security	Xiid
Xylem	Zimperium	Zscaler			

What can customers do?

Minimum Viable Secure Product

A minimum security baseline for enterprise-ready products and services

mvsp.dev

CISA'S STRATEGY

ESTABLISH CISA'S ROLE

COLLECT DATA AND BEST PRACTICES

DRIVE ADOPTION OF SECURE BY DESIGN BEST PRACTICES

YOUR NEXT STEPS

REVIEW

whitepaper and documentation

DISCUSS

history of safety in other fields

CONNECT

reach out to us and share

DRIVE

secure by design and secure by default

BUILD ROADMAPS

GATHER METRICS

ENGAGE STAKEHOLDERS

MORE INFO https://www.cisa.gov/securebydesign SecureByDesign@cisa.dhs.gov

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

LEARN MORE

https://www.cisa.gov/securebydesign

CONTACT US

SecureByDesign@cisa.dhs.gov
william.hicks@cisa.dhs.gov
cisaregion9outreach@cisa.dhs.gov