#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PNG-R02**

Dangerous: Critical Conversations About CISA's "Bad Practices"

Don Benack

Deputy Associate Director, Vuln Mgmt.
Cyber and Infrastructure Security Agency
@rm_sbin_sh

Josh Corman

(formerly) Chief Strategist, COVID-19 Task Force
Founder, I am the Cavalry
@joshcorman

Disclaimer

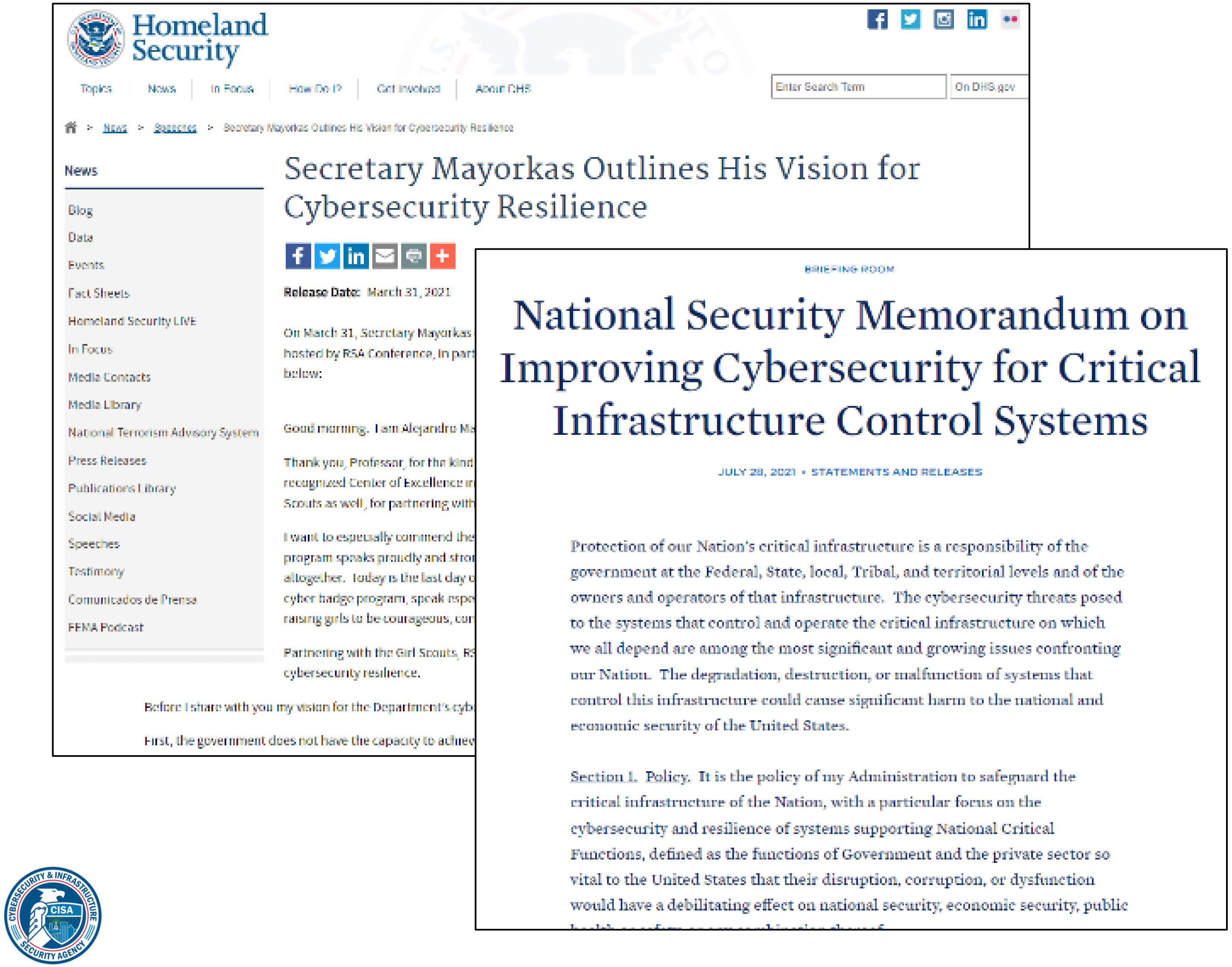
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The lead-up to Bad Practices

COVID TF
CARES Act
Operation Warp Speed

The lead-up to Bad Practices



Homeland Security

News > Speeches > Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience

Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience

Release Date: March 31, 2021

On March 31, Secretary Mayorkas
hosted by RSA Conference, In part
below:

Good morning. I am Alejandro Ma

Thank you, Professor, for the kind
recognized Center of Excellence in
Scouts as well, for partnering with

I want to especially commend the
program speaks proudly and stron
altogether. Today is the last day o
cyber badge program, speak espe
raising girls to be courageous, con

Partnering with the Girl Scouts, RS
cybersecurity resilience.

Before I share with you my vision for the Department's cybe

First, the government does not have the capacity to achiev

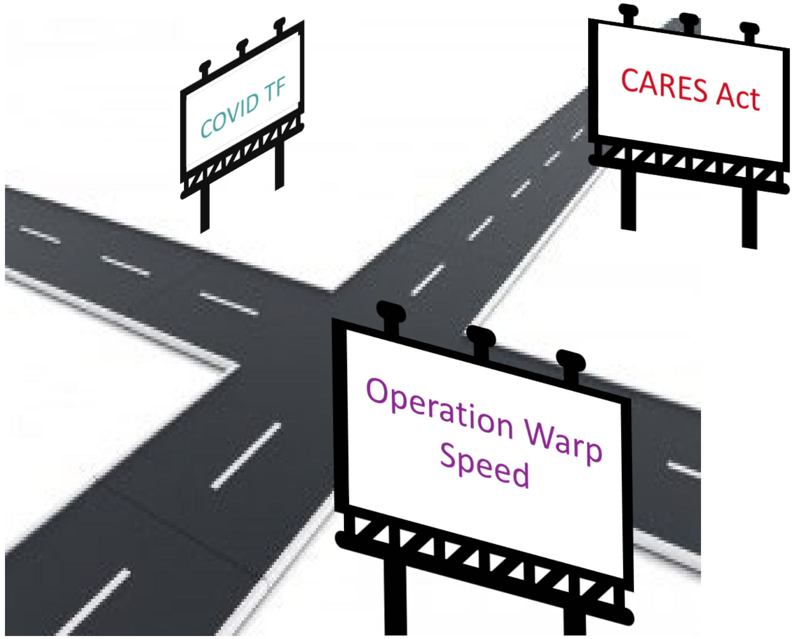
BRIEFING ROOM

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

JULY 28, 2021 • STATEMENTS AND RELEASES

Protection of our Nation's critical infrastructure is a responsibility of the government at the Federal, State, local, Tribal, and territorial levels and of the owners and operators of that infrastructure. The cybersecurity threats posed to the systems that control and operate the critical infrastructure on which we all depend are among the most significant and growing issues confronting our Nation. The degradation, destruction, or malfunction of systems that control this infrastructure could cause significant harm to the national and economic security of the United States.

Section 1. Policy. It is the policy of my Administration to safeguard the critical infrastructure of the Nation, with a particular focus on the cybersecurity and resilience of systems supporting National Critical Functions, defined as the functions of Government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof.

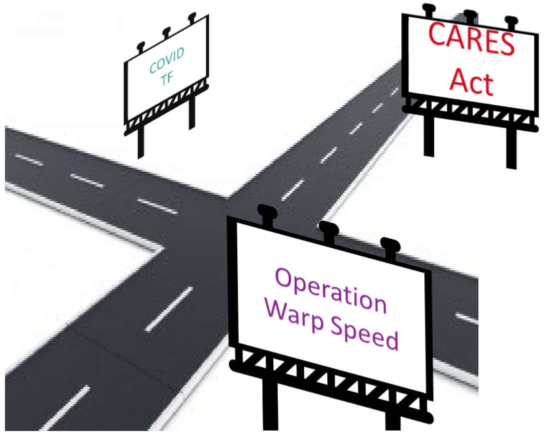


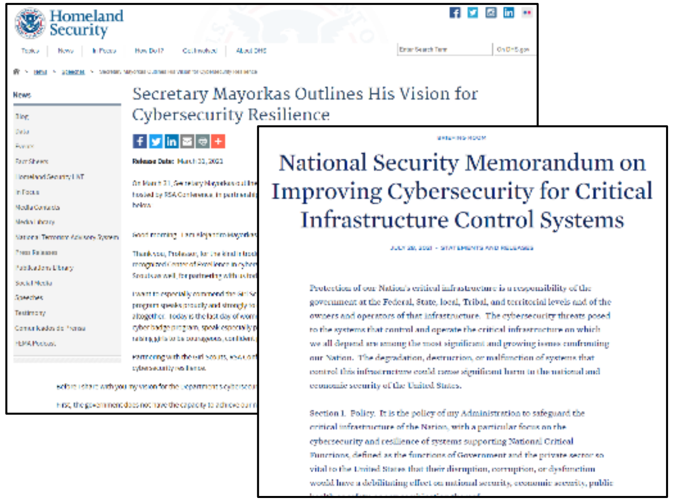
The lead-up to Bad Practices

Samuel Corum, Bloomberg

Chris Urso, Tampa Bay Times

Michael Ciaglo, Bloomberg, Getty Images





Homeland Security

Topics | News | In Focus | How Do I? | Get Involved | About DHS

News

Blog
Data
Events
Fact Sheets
Homeland Security LIVE
In Focus
Media Contacts
Media Library
National Terrorism Advisory System
Press Releases
Publications Library
Social Media
Speeches
Testimony
Comunicados de Prensa
FEMA Podcast

Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience

Release Date: March 31, 2021

BRIEFING ROOM

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

JULY 28, 2021 • STATEMENTS AND RELEASES

Protection of our Nation's critical infrastructure is a responsibility of the government at the Federal, State, local, Tribal, and territorial levels and of the owners and operators of that infrastructure. The cybersecurity threats posed to the systems that control and operate the critical infrastructure on which we all depend are among the most significant and growing issues confronting our Nation. The degradation, destruction, or malfunction of systems that control this infrastructure could cause significant harm to the national and economic security of the United States.

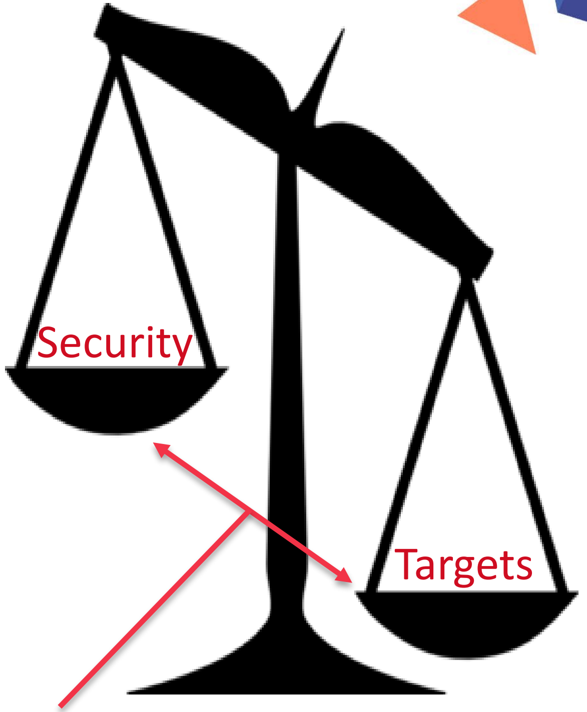
Section 1. Policy. It is the policy of my Administration to safeguard the critical infrastructure of the Nation, with a particular focus on the cybersecurity and resilience of systems supporting National Critical Functions, defined as the functions of Government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on national security, economic security, public

The lead-up to Bad Practices

Realization of some uncomfortable truths

- Many (most even) organizations are ***target rich*** and ***cyber poor***
- Widespread willingness to accept dangerous risk

© Mediadrumimages / @dzulfikri72



Potential risk disconnect

May lead to

The philosophy behind Bad Practices

Or, what a Bad Practice is (and isn't)

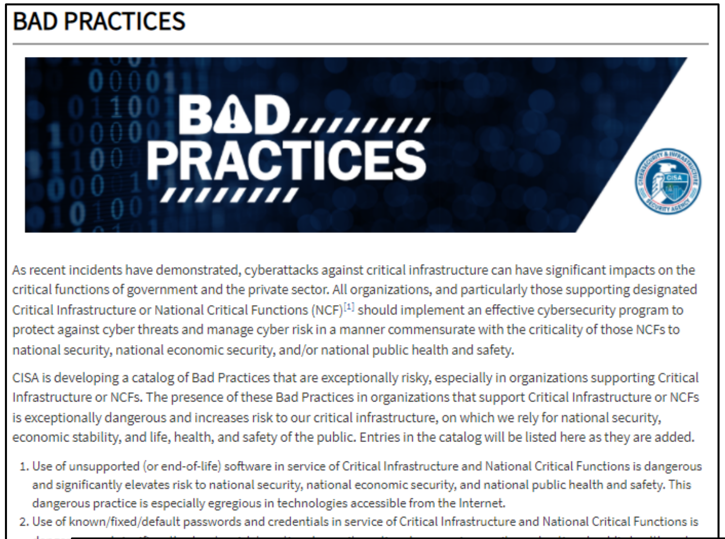
- Unimpeachably dangerous
- Not simply the opposite of a good or best practice
- The most simple, easy to digest and direct guidance we can provide

Bad Practice

DO NOT SNIFF BLUE PIT VIPERS.

The Bad Practices

- Use of unsupported (or end-of-life) software
- Use of known/fixed/default passwords and credentials
- Use of single-factor authentication for remote or administrative access



BAD PRACTICES

As recent incidents have demonstrated, cyberattacks against critical infrastructure can have significant impacts on the critical functions of government and the private sector. All organizations, and particularly those supporting designated Critical Infrastructure or National Critical Functions (NCF)[1] should implement an effective cybersecurity program to protect against cyber threats and manage cyber risk in a manner commensurate with the criticality of those NCFs to national security, national economic security, and/or national public health and safety.

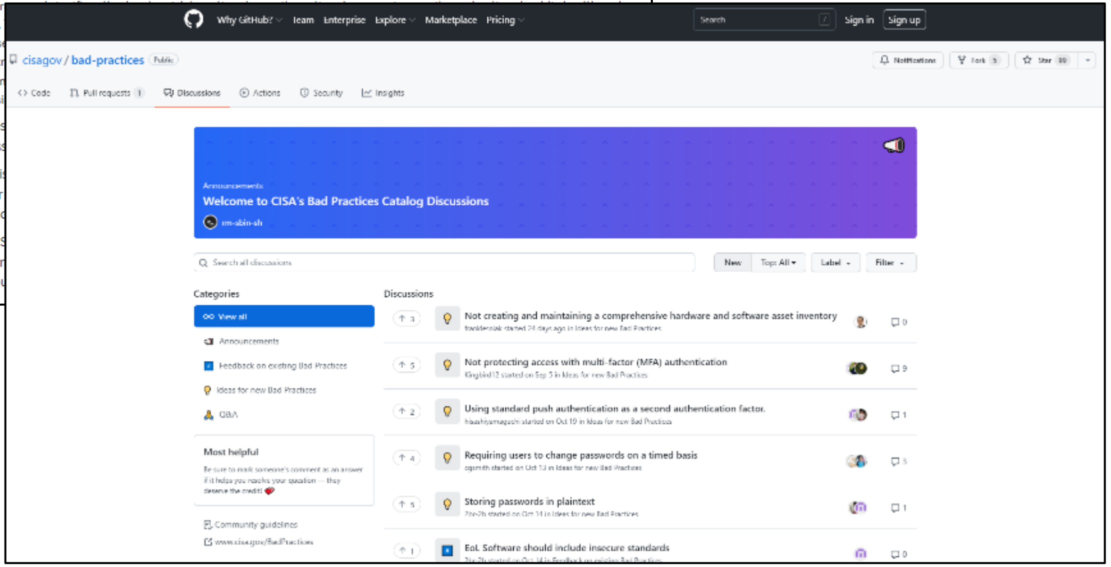
CISA is developing a catalog of Bad Practices that are exceptionally risky, especially in organizations supporting Critical Infrastructure or NCFs. The presence of these Bad Practices in organizations that support Critical Infrastructure or NCFs is exceptionally dangerous and increases risk to our critical infrastructure, on which we rely for national security, economic stability, and life, health, and safety of the public. Entries in the catalog will be listed here as they are added.

1. Use of unsupported (or end-of-life) software in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.
2. Use of known/fixed/default passwords and credentials in service of Critical Infrastructure and National Critical Functions is
danger
safety.
3. The us
Infrastr
econor
accessi

While thes
the necess

*This list i
particular
present ac

On our CIS
profession
gather you



cisagov / bad-practices Public

Announcements

Welcome to CISA's Bad Practices Catalog Discussions

rm-abin-sh

Categories

- View all
- Announcements
- Feedback on existing Bad Practices
- Ideas for new Bad Practices
- Q&A

Most helpful

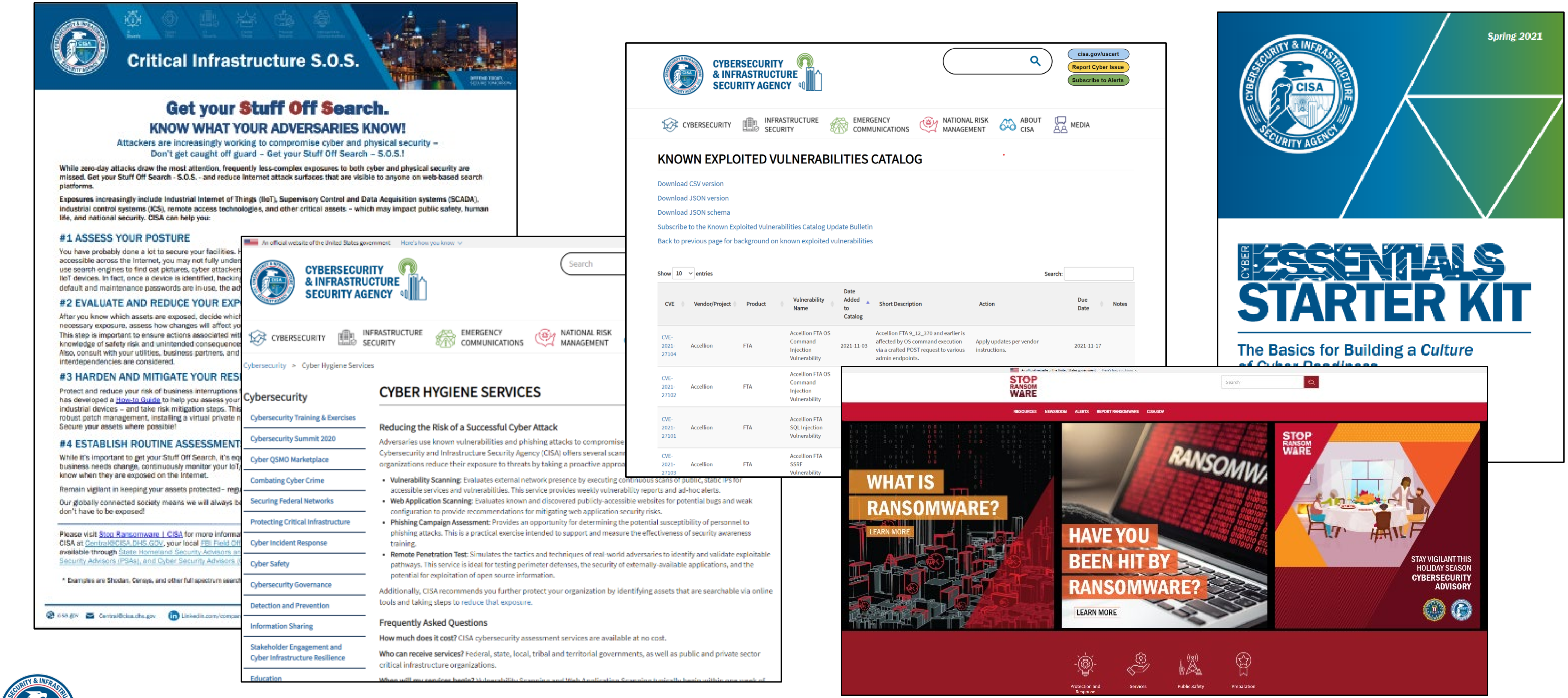
Be sure to mark someone's comment as an answer if it helps you resolve your question — they deserve the credit! ❤

- Community guidelines
- www.cisa.gov/BadPractices

Discussions

↑ 3	Not creating and maintaining a comprehensive hardware and software asset inventory frankdenniak started 24 days ago in Ideas for new Bad Practices	0
↑ 5	Not protecting access with multi-factor (MFA) authentication Kingbird12 started on Sep 5 in Ideas for new Bad Practices	9
↑ 2	Using standard push authentication as a second authentication factor. hisashiyamaguchi started on Oct 19 in Ideas for new Bad Practices	1
↑ 4	Requiring users to change passwords on a timed basis cgsmith started on Oct 13 in Ideas for new Bad Practices	5
↑ 5	Storing passwords in plaintext 2hr-2h started on Oct 14 in Ideas for new Bad Practices	1
↑ 1	EoL Software should include insecure standards 2hr-2h started on Oct 14 in Feedback on existing Bad Practices	0

Bad Practices are part of a wider effort



Critical Infrastructure S.O.S.

Get your Stuff Off Search.

KNOW WHAT YOUR ADVERSARIES KNOW!

Attackers are increasingly working to compromise cyber and physical security – Don't get caught off guard – Get your Stuff Off Search – S.O.S.!

While zero-day attacks draw the most attention, frequently less-complex exposures to both cyber and physical security are missed. Get your Stuff Off Search - S.O.S. - and reduce Internet attack surfaces that are visible to anyone on web-based search platforms.

Exposures increasingly include Industrial Internet of Things (IIoT), Supervisory Control and Data Acquisition systems (SCADA), industrial control systems (ICS), remote access technologies, and other critical assets – which may impact public safety, human life, and national security. CISA can help you:

#1 ASSESS YOUR POSTURE

You have probably done a lot to secure your facilities. H accessible across the Internet, you may not fully under use search engines to find cat pictures, cyber attacker IIoT devices. In fact, once a device is identified, hacking default and maintenance passwords are in-use, the ad

#2 EVALUATE AND REDUCE YOUR EXP

After you know which assets are exposed, decide which necessary exposure, assess how changes will affect yo This step is important to ensure actions associated wit knowledge of safety risk and unintended consequence Also, consult with your utilities, business partners, and interdependencies are considered.

#3 HARDEN AND MITIGATE YOUR RES

Protect and reduce your risk of business interruptions has developed a How-to Guide to help you assess your industrial devices – and take risk mitigation steps. This robust patch management, installing a virtual private n Secure your assets where possible!

#4 ESTABLISH ROUTINE ASSESSMENT

While it's important to get your Stuff Off Search, it's eq business needs change, continuously monitor your IoT, know when they are exposed on the Internet.

Remain vigilant in keeping your assets protected – regu

Our globally connected society means we will always be don't have to be exposed!

Please visit Stop Ransomware | CISA for more informa CISA at Central@CISA.DHS.GOV, your local FBI Field Off available through State Homeland Security Advisors an Security Advisors (PSAs), and Cyber Security Advisors (

* Examples are Shodan, Censys, and other full spectrum search

cisa.gov Central@cisa.dhs.gov LinkedIn.com/compan

An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT

Cybersecurity > Cyber Hygiene Services

Cybersecurity

- Cybersecurity Training & Exercises
- Cybersecurity Summit 2020
- Cyber QSMO Marketplace
- Combating Cyber Crime
- Securing Federal Networks
- Protecting Critical Infrastructure
- Cyber Incident Response
- Cyber Safety
- Cybersecurity Governance
- Detection and Prevention
- Information Sharing
- Stakeholder Engagement and Cyber Infrastructure Resilience
- Education

CYBER HYGIENE SERVICES

Reducing the Risk of a Successful Cyber Attack

Adversaries use known vulnerabilities and phishing attacks to compromise Cybersecurity and Infrastructure Security Agency (CISA) offers several scann organizations reduce their exposure to threats by taking a proactive approa

- **Vulnerability Scanning:** Evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- **Web Application Scanning:** Evaluates known and discovered publicly-accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.
- **Phishing Campaign Assessment:** Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training.
- **Remote Penetration Test:** Simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally-available applications, and the potential for exploitation of open source information.

Additionally, CISA recommends you further protect your organization by identifying assets that are searchable via online tools and taking steps to reduce that exposure.

Frequently Asked Questions

How much does it cost? CISA cybersecurity assessment services are available at no cost.

Who can receive services? Federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations.

When will my services begin? Vulnerability Scanning and Web Application Scanning typically begin within one week of

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

cisa.gov/uscert

Report Cyber Issue

Subscribe to Alerts

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

KNOWN EXPLOITED VULNERABILITIES CATALOG

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities

Show 10 entries

Search:

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2021-27104	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability	2021-11-03	Accellion FTA 9_12_370 and earlier is affected by OS command execution via a crafted POST request to various admin endpoints.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-27102	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability					
CVE-2021-27101	Accellion	FTA	Accellion FTA SQL Injection Vulnerability					
CVE-2021-27103	Accellion	FTA	Accellion FTA SSRF Vulnerability					

Spring 2021

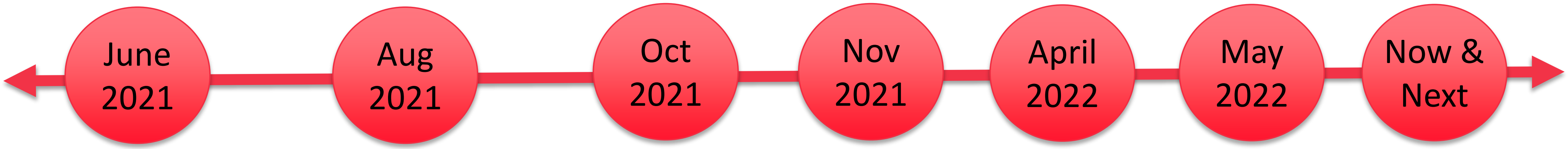
CYBER ESSENTIALS STARTER KIT

The Basics for Building a Culture of Cyber Readiness

STOP RANSOMWARE

WHAT IS RANSOMWARE?
LEARN MORE
HAVE YOU BEEN HIT BY RANSOMWARE?
LEARN MORE
STOP RANSOMWARE
STAY VIGILANT THIS HOLIDAY SEASON CYBERSECURITY ADVISORY

Moving Beyond the Prologue



June 2021

CISA Publishes first two Bad Practices

Aug 2021

White House Insurance Industry Meeting

Bad Practices Forum on GitHub Third Bad Practice Published

Oct 2021

CISA Summit 2021

Nov 2021

BOD 22-01 Known Exploited Vulns

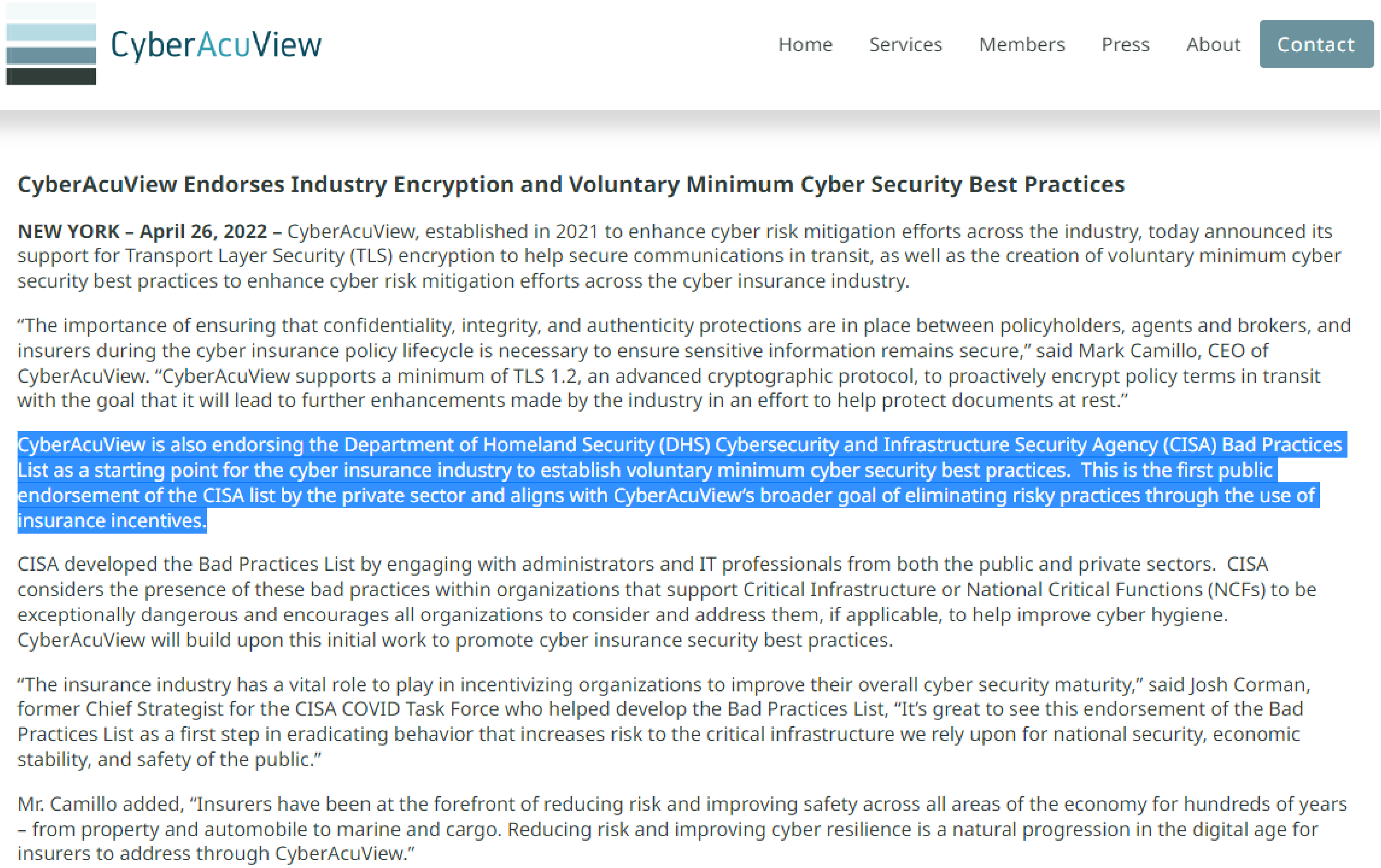
April 2022

CyberAcuView Endorses CISA Bad Practices

May 2022

Bad Practices in Senate Testimony

Now & Next



CyberAcuView Endorses Industry Encryption and Voluntary Minimum Cyber Security Best Practices

NEW YORK – April 26, 2022 – CyberAcuView, established in 2021 to enhance cyber risk mitigation efforts across the industry, today announced its support for Transport Layer Security (TLS) encryption to help secure communications in transit, as well as the creation of voluntary minimum cyber security best practices to enhance cyber risk mitigation efforts across the cyber insurance industry.

"The importance of ensuring that confidentiality, integrity, and authenticity protections are in place between policyholders, agents and brokers, and insurers during the cyber insurance policy lifecycle is necessary to ensure sensitive information remains secure," said Mark Camillo, CEO of CyberAcuView. "CyberAcuView supports a minimum of TLS 1.2, an advanced cryptographic protocol, to proactively encrypt policy terms in transit with the goal that it will lead to further enhancements made by the industry in an effort to help protect documents at rest."

CyberAcuView is also endorsing the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Bad Practices List as a starting point for the cyber insurance industry to establish voluntary minimum cyber security best practices. This is the first public endorsement of the CISA list by the private sector and aligns with CyberAcuView's broader goal of eliminating risky practices through the use of insurance incentives.

CISA developed the Bad Practices List by engaging with administrators and IT professionals from both the public and private sectors. CISA considers the presence of these bad practices within organizations that support Critical Infrastructure or National Critical Functions (NCFs) to be exceptionally dangerous and encourages all organizations to consider and address them, if applicable, to help improve cyber hygiene. CyberAcuView will build upon this initial work to promote cyber insurance security best practices.

"The insurance industry has a vital role to play in incentivizing organizations to improve their overall cyber security maturity," said Josh Corman, former Chief Strategist for the CISA COVID Task Force who helped develop the Bad Practices List, "It's great to see this endorsement of the Bad Practices List as a first step in eradicating behavior that increases risk to the critical infrastructure we rely upon for national security, economic stability, and safety of the public."

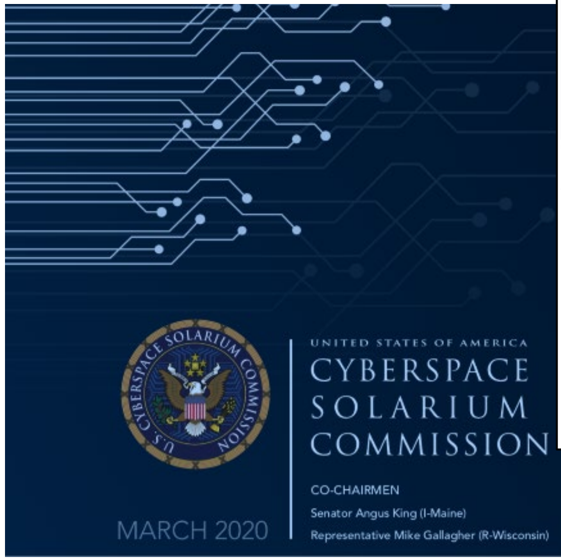
Mr. Camillo added, "Insurers have been at the forefront of reducing risk and improving safety across all areas of the economy for hundreds of years – from property and automobile to marine and cargo. Reducing risk and improving cyber resilience is a natural progression in the digital age for insurers to address through CyberAcuView."

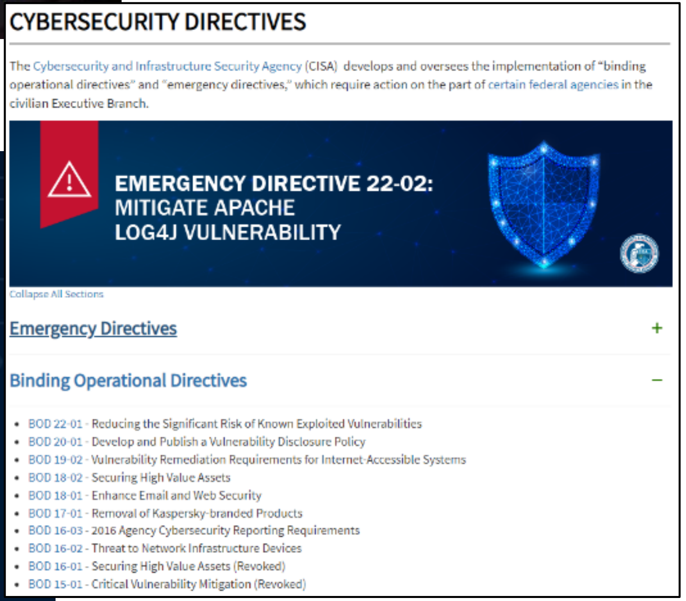
Play (k)
1:29 / 5:29
MR. CORMAN

Upcoming actions from CISA

- Encourage the community to organize and act
- Meet with all sector risk management agencies
- Link funding opportunities to eradication of bad practices
- Update the Cyber Essentials
- Add to Bad Practices

Don't try to frighten us with your sorcerer's ways, Lord Vader.


U.S. CYBERSPACE SOLARIUM COMMISSION
UNITED STATES OF AMERICA
CYBERSPACE SOLARIUM COMMISSION
CO-CHAIRMEN
Senator Angus King (I-Maine)
Representative Mike Gallagher (R-Wisconsin)
MARCH 2020



CYBERSECURITY DIRECTIVES

The Cybersecurity and Infrastructure Security Agency (CISA) develops and oversees the implementation of "binding operational directives" and "emergency directives," which require action on the part of certain federal agencies in the civilian Executive Branch.

EMERGENCY DIRECTIVE 22-02: MITIGATE APACHE LOG4J VULNERABILITY
Collapse All Sections

Emergency Directives +

Binding Operational Directives –

- BOD 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities
- BOD 20-01 - Develop and Publish a Vulnerability Disclosure Policy
- BOD 19-02 - Vulnerability Remediation Requirements for Internet-Accessible Systems
- BOD 18-02 - Securing High Value Assets
- BOD 18-01 - Enhance Email and Web Security
- BOD 17-01 - Removal of Kaspersky-branded Products
- BOD 16-03 - 2016 Agency Cybersecurity Reporting Requirements
- BOD 16-02 - Threat to Network Infrastructure Devices
- BOD 16-01 - Securing High Value Assets (Revoked)
- BOD 15-01 - Critical Vulnerability Mitigation (Revoked)

Your implementation: next week

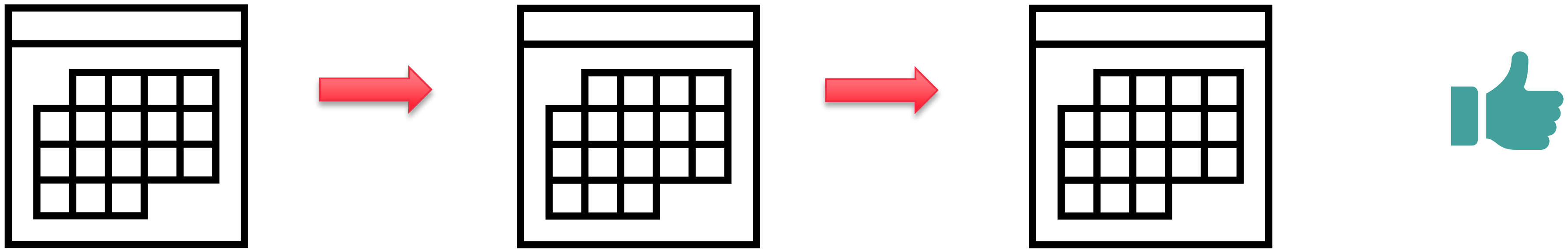
- Review the Bad Practices with your C-Suite
- Contribute to the conversation and development: https://github.com/cisagov/bad-practices/discussions
- Get your Stuff off Search: https://www.cisa.gov/publication/stuff-off-search
- Use free CISA services to manage your Cyber Hygiene: https://www.cisa.gov/cyber-hygiene-services
- Connect with local CISA resources in your region https://www.cisa.gov/cisa-regions

2022

Jun 13

Your implementation: within three months

- Establish policies prohibiting implementation of Bad Practices
- Develop plans to eradicate Bad Practices in your organization
- Use the Known Exploited Vulnerabilities Catalog prioritize patching: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Review your program against the Cyber Essentials: https://www.cisa.gov/cyber-essentials



June

July

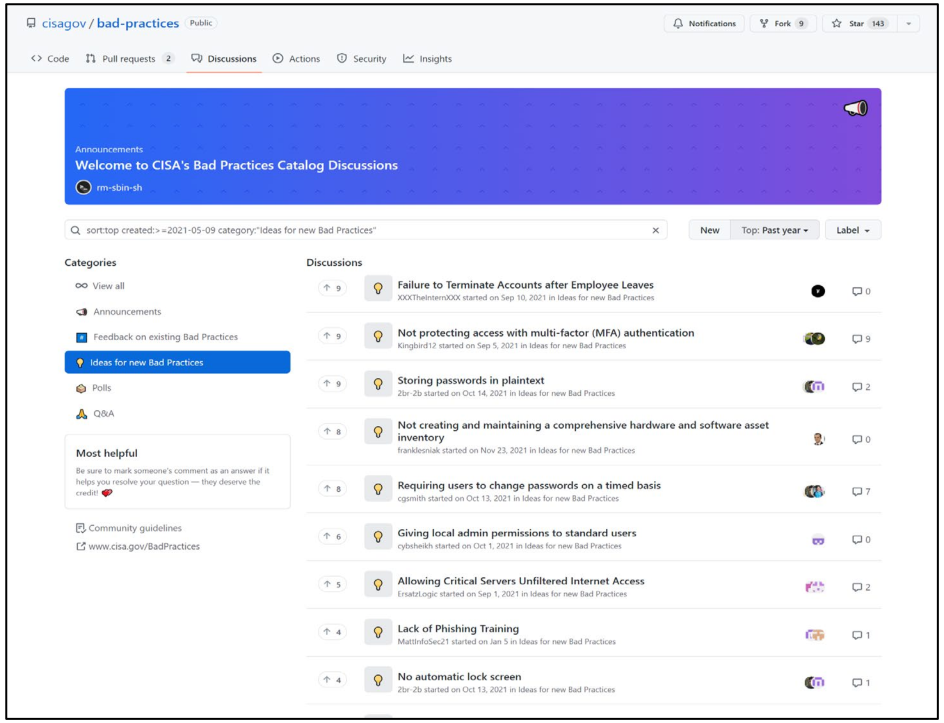
August

Your implementation: within six months

- Routinely mitigate Known Exploited Vulnerabilities swiftly
- Begin eliminating Bad Practices and implementing Cyber Essentials
- Talk to your Vendors, Insurer and maybe even your Regulator
- Explore modern defensible architectures

There’s More to Come

- CISA is considering additional Bad Practice Candidates
  - Internet Exposed Administrative Services?
  - Recalled products in Production Environments?
  - Failure to Segment/Separate Privilege?



Announcements

Welcome to CISA's Bad Practices Catalog Discussions

rm-sbin-sh

sort:top created:>=2021-05-09 category:"Ideas for new Bad Practices"

Categories

- View all
- Announcements
- Feedback on existing Bad Practices
- Ideas for new Bad Practices
- Polls
- Q&A

Most helpful

Be sure to mark someone’s comment as an answer if it helps you resolve your question — they deserve the credit! ❤

Community guidelines

www.cisa.gov/BadPractices

Discussions

↑ 9 Failure to Terminate Accounts after Employee Leaves
XXXTheInternXXX started on Sep 10, 2021 in Ideas for new Bad Practices — 0

↑ 9 Not protecting access with multi-factor (MFA) authentication
Kingbird12 started on Sep 5, 2021 in Ideas for new Bad Practices — 9

↑ 9 Storing passwords in plaintext
2br-2b started on Oct 14, 2021 in Ideas for new Bad Practices — 2

↑ 8 Not creating and maintaining a comprehensive hardware and software asset inventory
franklesniak started on Nov 23, 2021 in Ideas for new Bad Practices — 0

↑ 8 Requiring users to change passwords on a timed basis
cgsmith started on Oct 13, 2021 in Ideas for new Bad Practices — 7

↑ 6 Giving local admin permissions to standard users
cybsheikh started on Oct 1, 2021 in Ideas for new Bad Practices — 0

↑ 5 Allowing Critical Servers Unfiltered Internet Access
ErsatzLogic started on Sep 1, 2021 in Ideas for new Bad Practices — 2

↑ 4 Lack of Phishing Training
MattInfoSec21 started on Jan 5 in Ideas for new Bad Practices — 1

↑ 4 No automatic lock screen
2br-2b started on Oct 13, 2021 in Ideas for new Bad Practices — 1

- Your engagement is needed: https://github.com/cisagov/bad-practices/discussions

Questions and Answers Opportunity

- Let’s Talk
  - What opportunities do you see?
  - What concerns do you have?
  - What dangerous practice should we address next?
  - How can we incentivize and motivate action?

- Didn’t get a chance to ask your question or share your thought?
  - email: vulnerability@cisa.dhs.gov with subject line: Bad Practices
  - GitHub: https://github.com/cisagov/bad-practices/discussions

Backup References

- Pragmatic Cyber Security Webinar | CISA
  https://www.cisa.gov/pragmatic-cyber-security-webinar
- CISA Insights: Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm (October 2021)
  https://www.cisa.gov/insights
- Senate Testimony
  https://youtube.com/playlist?list=PLSNVlMw4ldTw6QqXlNvSNn-b9A8aM93vu
- Stop Ransomware | CISA
  https://www.cisa.gov/stopransomware