

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

**“DEFEND TODAY,
SECURE TOMORROW.”**

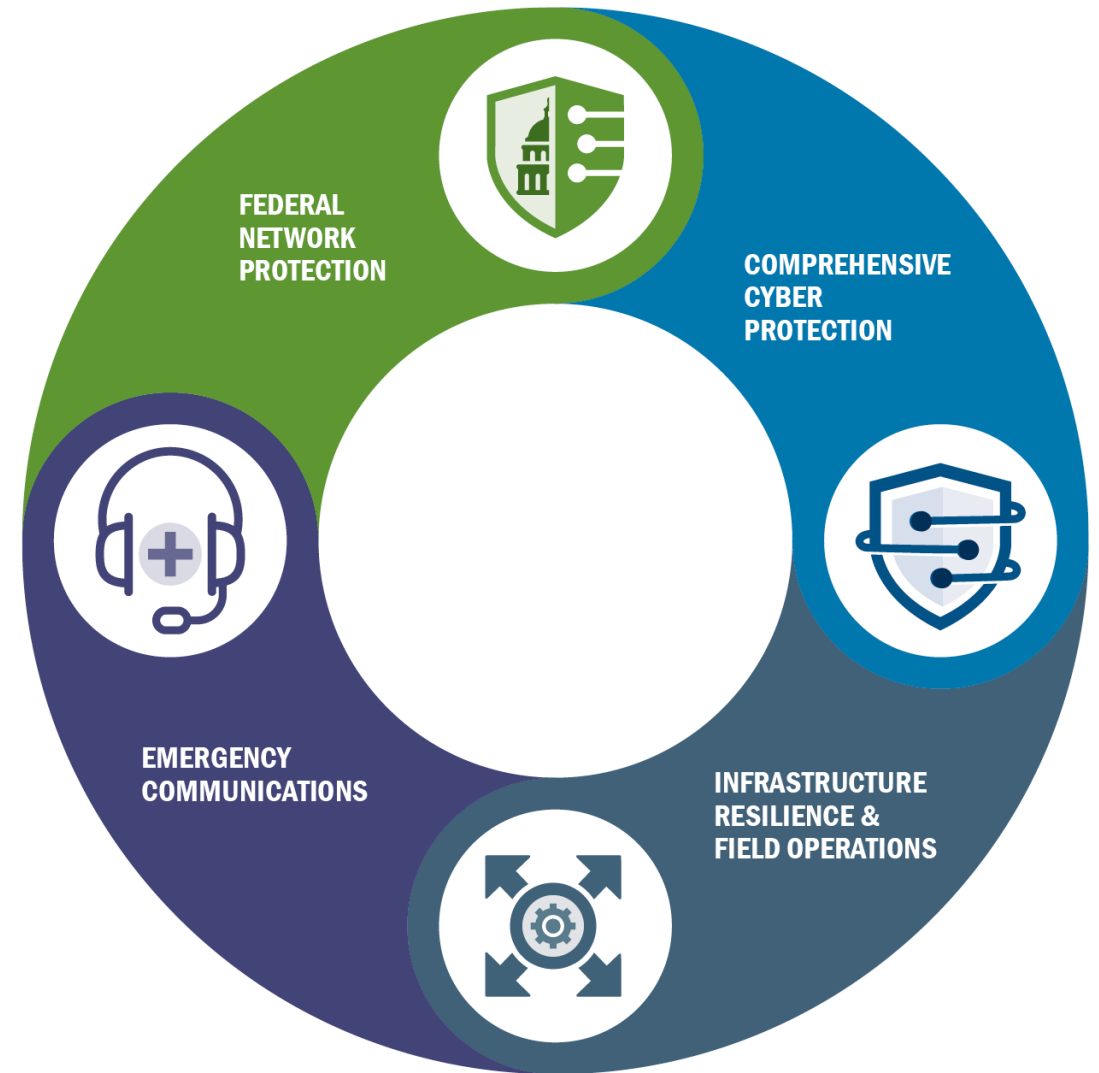


Josh Corman, Healthcare Strategist, CISA COVID Task Force
July 14, 2021

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

We are the Nation's Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient
infrastructure for the
American people.

MISSION

CISA partners with industry and
government to understand and
manage risk to our Nation's
critical infrastructure.



OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent
threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical
infrastructure and
address long-term risks

months | years | decades

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

**CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**

CYBERSECURITY

INFRASTRUCTURE SECURITY

EMERGENCY COMMUNICATIONS

NATIONAL RESILIENCE MANAGEMENT

Cybersecurity > Ransomware

Cybersecurity

Cybersecurity Training & Exercises

Cybersecurity Summit 2020

Cyber QSMO Marketplace

Combating Cyber Crime

Securing Federal Networks

Protecting Critical Infrastructure

Cyber Incident Response

RANSOMWARE GUIDANCE AND RESOURCES

Ransomware is an ever-evolving form of malware designed to encrypt systems that rely on them unusable. Malicious actors then demand r



THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

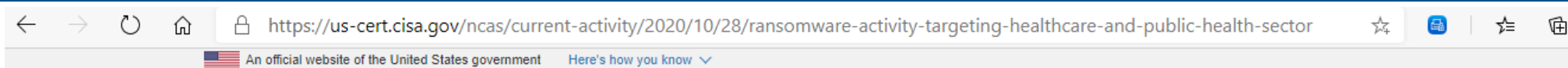
Under President Biden's leadership, the Federal Government is stepping up to do its' part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. But there are immediate steps you can take to protect yourself, as well as your customers and the broader economy. Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft, we urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat.

The most important takeaway from the recent spate of ransomware attacks on U.S., Irish, German and other organizations around the world is that companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively. To understand your risk, business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you have the ability to continue or quickly restore operations.



Recent Healthcare Delivery Attacks



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



Services

Report

[Alerts and Tips](#)

[Resources](#)

[Industrial Control Systems](#)

[National Cyber Awareness System](#) > [Current Activity](#) > [Ransomware Activity Targeting the Healthcare and Public Health Sector](#)

Ransomware Activity Targeting the Healthcare and Public Health Sector

Original release date: October 28, 2020



The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the U.S. Department of Health and Human Services (HHS) have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.

CISA, FBI, and HHS have released [AA20-302A Ransomware Activity Targeting the Healthcare and Public Health Sector](#) that details both the threat and practices that healthcare organizations should continuously engage in to help manage the risk posed by ransomware and other cyber threats. The advisory references the [joint CISA MS-ISAC Ransomware Guide](#) that provides a ransomware response checklist that can serve as a ransomware-specific addendum to organization cyber incident response plans.

CISA, FBI, and HHS are sharing this information in order to provide a warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats. CISA encourages users and administrators to review CISA's [Ransomware webpage](#) for additional information.

Latest Alerts

[Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data](#)

Friday, October 30, 2020

[Ransomware Activity Targeting the Healthcare and Public Health Sector](#)

Wednesday, October 28, 2020

[North Korean Advanced Persistent Threat Focus: Kimsuky](#)

Tuesday, October 27, 2020

[More Alerts »](#)

Recent Vulnerabilities



TARGET RICH CYBER POOR

Information • Incentives • Resources



5 best practices from the White House memo:

1. Back up your data, system images, and configurations; then regularly test them and keep the backups offline
2. Update and patch systems promptly
3. Test your Incident Response Plan
4. Check your security team's work
5. Segment your networks




Other High Impact Measures You Can Take:

- multifactor authentication (because passwords alone are routinely compromised)
- endpoint detection & response (to hunt for malicious activity on a network and block it)
- encryption (so if data is stolen, it is unusable)
- a skilled, empowered security team (to patch rapidly, and share and incorporate threat information in your defenses).







**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**


COVID Questions

Report Cyber Issue

CYBERSECURITY

INFRASTRUCTURE SECURITY


EMERGENCY COMMUNICATIONS

NATIONAL RISK MANAGEMENT

ABOUT CISA

MEDIA

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 internet-accessible technologies.
2. Use of known/fixed/default passwords and credentials 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 internet-accessible technologies.

While these practices are dangerous for Critical Infrastructure and NCFs, CISA encourages all organizations to engage in the necessary actions and critical conversations to address Bad Practices.*

*This list is focused and does not include every possible inadvisable cybersecurity practice. The lack of inclusion of any particular cybersecurity practice does not indicate that CISA endorses such a practice or deems such a practice to present acceptable levels of risk.

How to Get Started:

- Cyber Hygiene Services*
- Cyber Resilience Review (CRR)
- Cyber Infrastructure Survey (CIS)
- External Dependencies Management Assessment (EDM)
- National Cyber Awareness System (NCAS)
- Advanced Malware Analysis Center (AMAC)
- Cyber Security Evaluation Tool (CSET)
- Risk and Vulnerability Assessment (RVA)
- Validated Architecture Design Review (VADR)
- Malicious Domain Blocking (via Center for Internet Security)**
- *Ransomware Readiness Assessment****
- *Stuff Off Search (SOS)****

Start Anywhere. Start Today. CISA Can Help.

*including Vulnerability Scanning, Web Application Scanning, Phishing Campaign Assessment, and Remote Penetration Test

**available to healthcare delivery organizations and SLTT

***pending/to be published

