CISA CYBERSECURITY RESOURCES

July 27, 2021

Greater New Jersey Motorcoach Association

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

FEDERAL NETWORK PROTECTION

COMPREHENSIVE CYBER PROTECTION

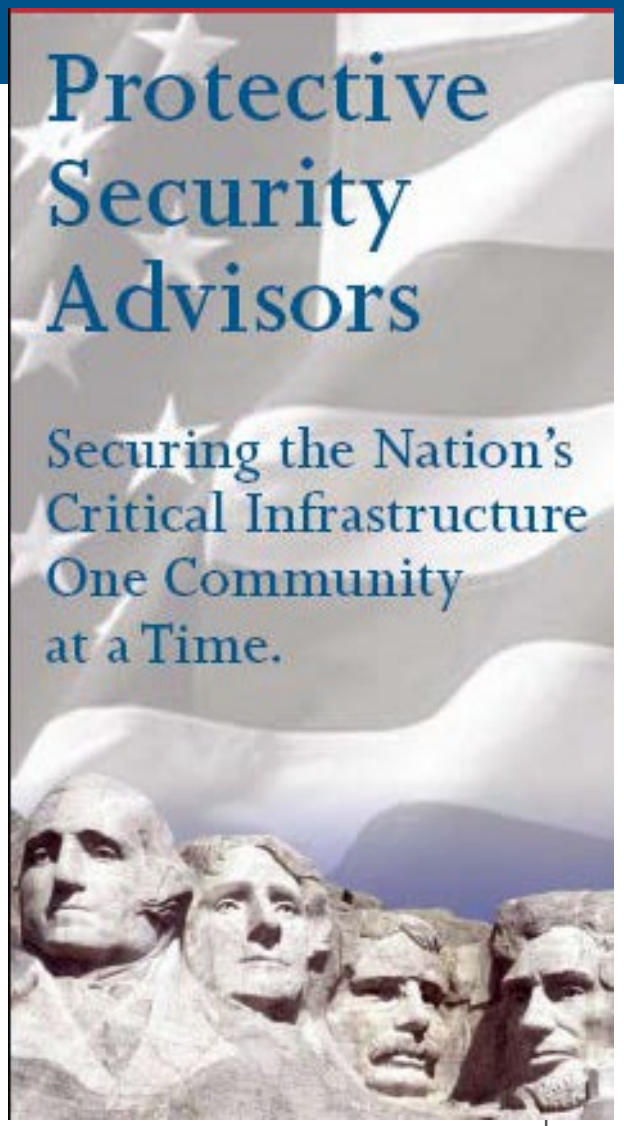
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS

EMERGENCY COMMUNICATIONS

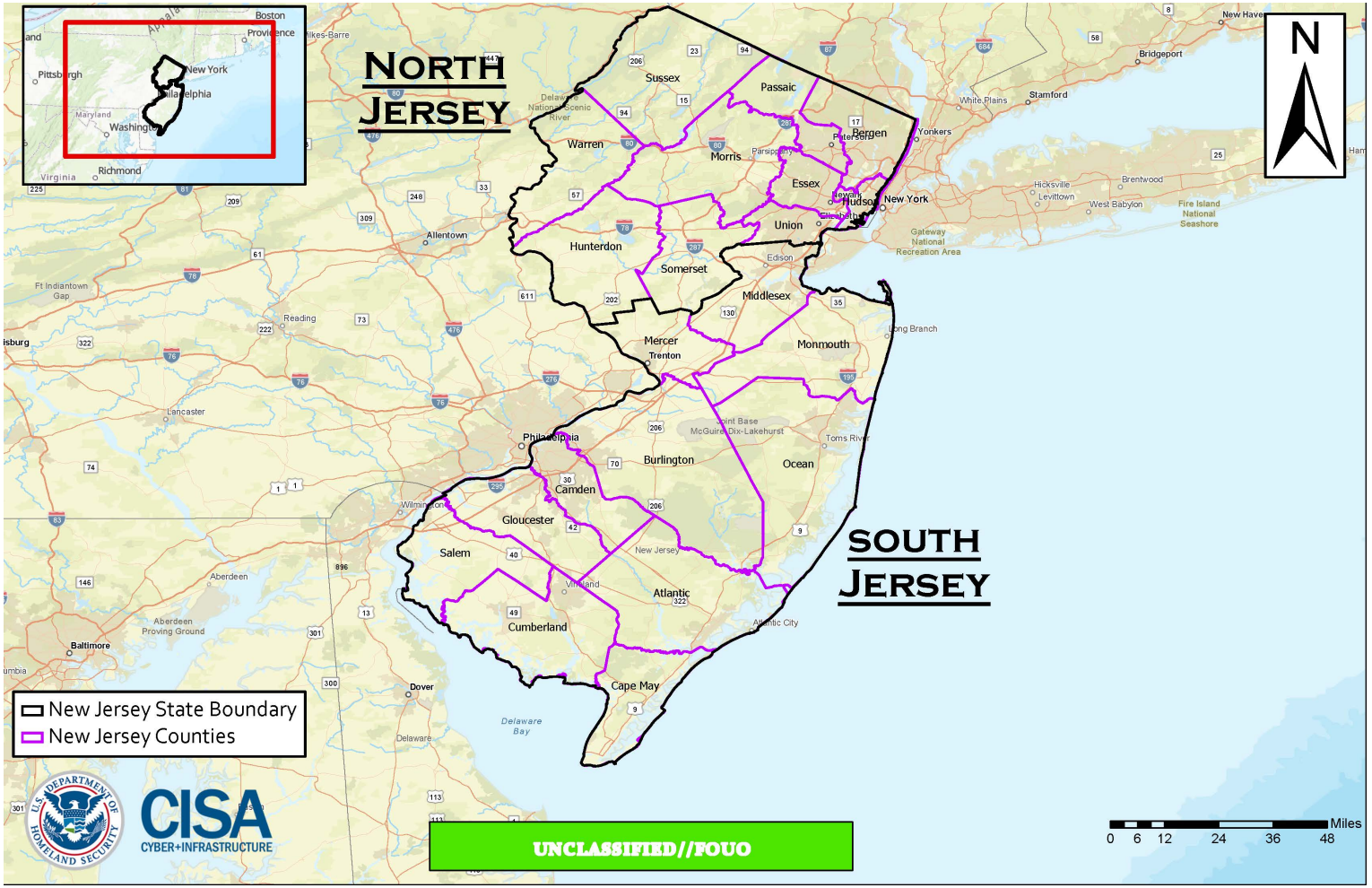
Protective Security Advisor

Assistance with

- Connecting you with your state & local partners.
  - Resources
  - Threat information
- Assessing vulnerabilities
- Exercises
- Training
  - Run Hide Fight
  - Recognizing suspicious activity
  - Bombing Prevention
- To contact your local PSA
  - Central@CISA.GOV



New Jersey PSA Districts



CISA NJ Based PSA & CSA contacts

PSA Dan Schultz
CISA NJ-North District
"NJ counties north of Mercer & Middlesex"

Contact Information:

Daniel.Schultz@hq.dhs.gov

202-538-5530

PSA Andrew Smith
CISA NJ-South District
"Everywhere else in the state"

Contact Information:

Andrew.Smith@hq.dhs.gov

202-875-1034

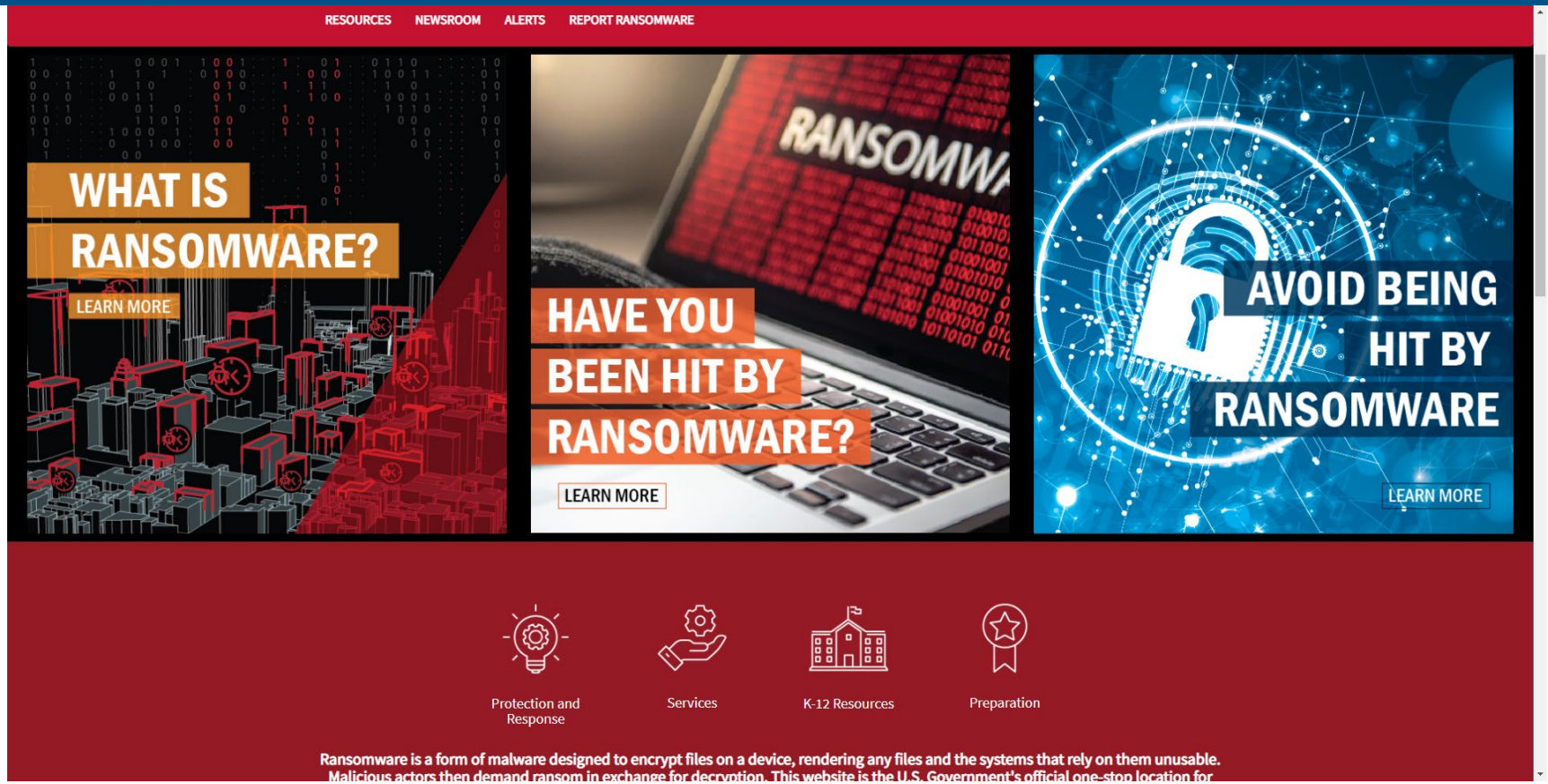
CSA Anthony Zissimos
CISA NJ

Contact Information:

anthony.zissimos@cisa.dhs.gov

202-948-1763

StopRansomware.Gov



Ransomware Resources

- Fact Sheets & Information
- Ransomware 101
- Ransomware Guide
- Services
- Training
- Webinars
- Bad Practices
- Campaigns
- Sector Risk Management Agencies

Cyber Hygiene Services

Free CISA scanning and testing services to help organizations assess, identify, and reduce their exposure to threats, including ransomware.

- This suite of services includes:
  - **Vulnerability Scanning:** Identifies externally-accessible assets and services that are vulnerable to common attacks.
  - **Web Application Scanning:** Identifies website weaknesses and poor configurations that attackers may exploit.
  - **Phishing Campaign Assessment:** Determines the susceptibility of an organization's personnel to opening malicious emails (i.e., phishing), which are a leading cause of ransomware.
  - **Remote Penetration Test:** Tests perimeter defenses by mimicking the techniques adversaries use to gain unauthorized access to networks

Cyber Security Evaluation Tool

CISA
CYBER+INFRASTRUCTURE

Ransomware Assessment Module

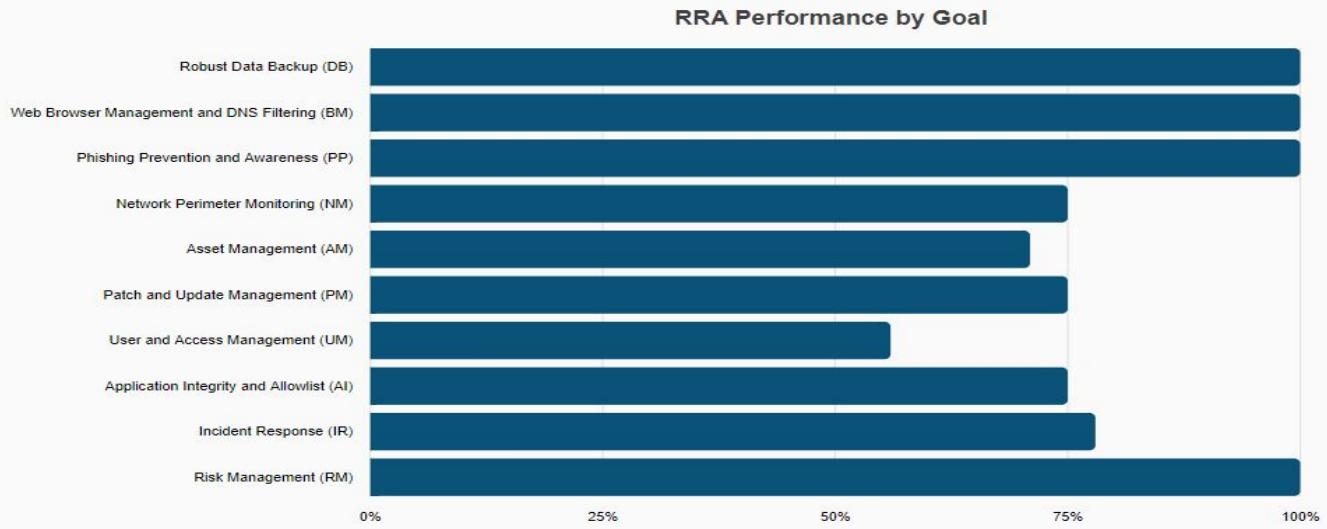
Ransomware Assessment Module

- Self-assessment module in Cybersecurity Evaluation Tool (CSET) v10.3
- 10 Goals with 48 tiered practices; 18 Basic, 16 Intermediate, 14 Advanced
  - Based off CISA Cyber Essentials, Ransomware Guide and leverages the MITRE ATT&CK Framework
  - Structured to give organizations a clear path for improvement
  - Complete with supplemental resources for each practice
- Several reports and charts depicting results
  - Ransomware Assessment Goal Report
  - Deficiency report highlighting weakest goals

Ransomware Assessment Goal Report

Prepare | Assessment | Results

Goal Performance



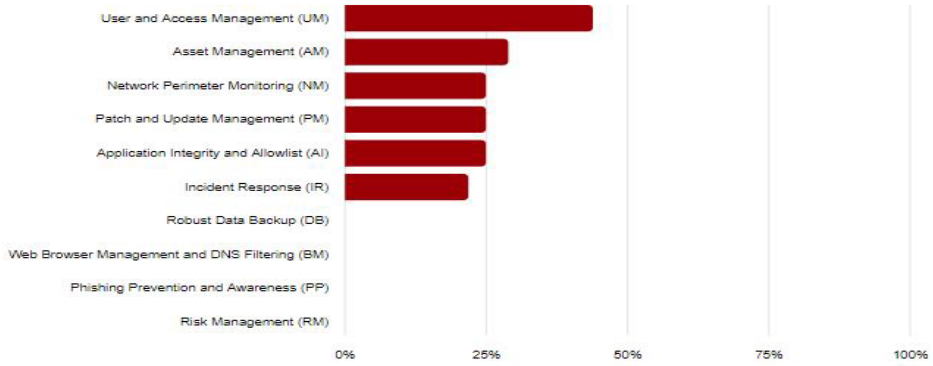
RRA Practice Scoring

	Yes	No	Unanswered	Total Practices	Percent Complete
Robust Data Backup (DB)	2	0	0	2	100.0%
Web Browser Management and DNS Filtering (BM)	2	0	0	2	100.0%
Phishing Prevention and Awareness (PP)	3	0	0	3	100.0%
Network Perimeter Monitoring (NM)	3	1	0	4	75.0%

Ransomware Assessment Deficiency Report

Suggested Areas for Improvement

The goals in the assessment are ranked in order of deficiency with goals having fewer satisfied practices ranked higher in the chart. The bar graph reflects the percentage of practices for each goal that are answered "No" or are left unanswered.



Deficiencies

Marked for Review -

NM:A.Q04	Has the organization established a baseline of network traffic and is it used to identify anomalous activity?	No
AM:A.Q04	Does the organization quarantine and/or remove all rogue hardware?	No
AM:A.Q07	Does the organization manage system configurations using security hardening guides?	No

Ransomware Assessment Resources

AI:I.Q03	Is the Allowlist organized by software publisher, and is that list used to allow only approved software to run on organizational systems?	NIST SP 800-167: Allowlisting: For more information on allowlists, this publication is intended to assist organizations in understanding the basics of application allowlisting. It also explains planning and implementation for allowlisting technologies throughout the security deployment lifecycle. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-7 (5) CIS Controls Version 8: The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.
AI:A.Q04	Has the organization documented a list of known approved software (an Allowlist) organized by software publisher and version number, and is that list used to allow only approved software to run on organizational systems?	NIST SP 800-167: Allowlisting: For more information on allowlists, this publication is intended to assist organizations in understanding the basics of application allowlisting. It also explains planning and implementation for allowlisting technologies throughout the security deployment lifecycle. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CM-7(5) CIS Controls Version 8: The CIS Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.

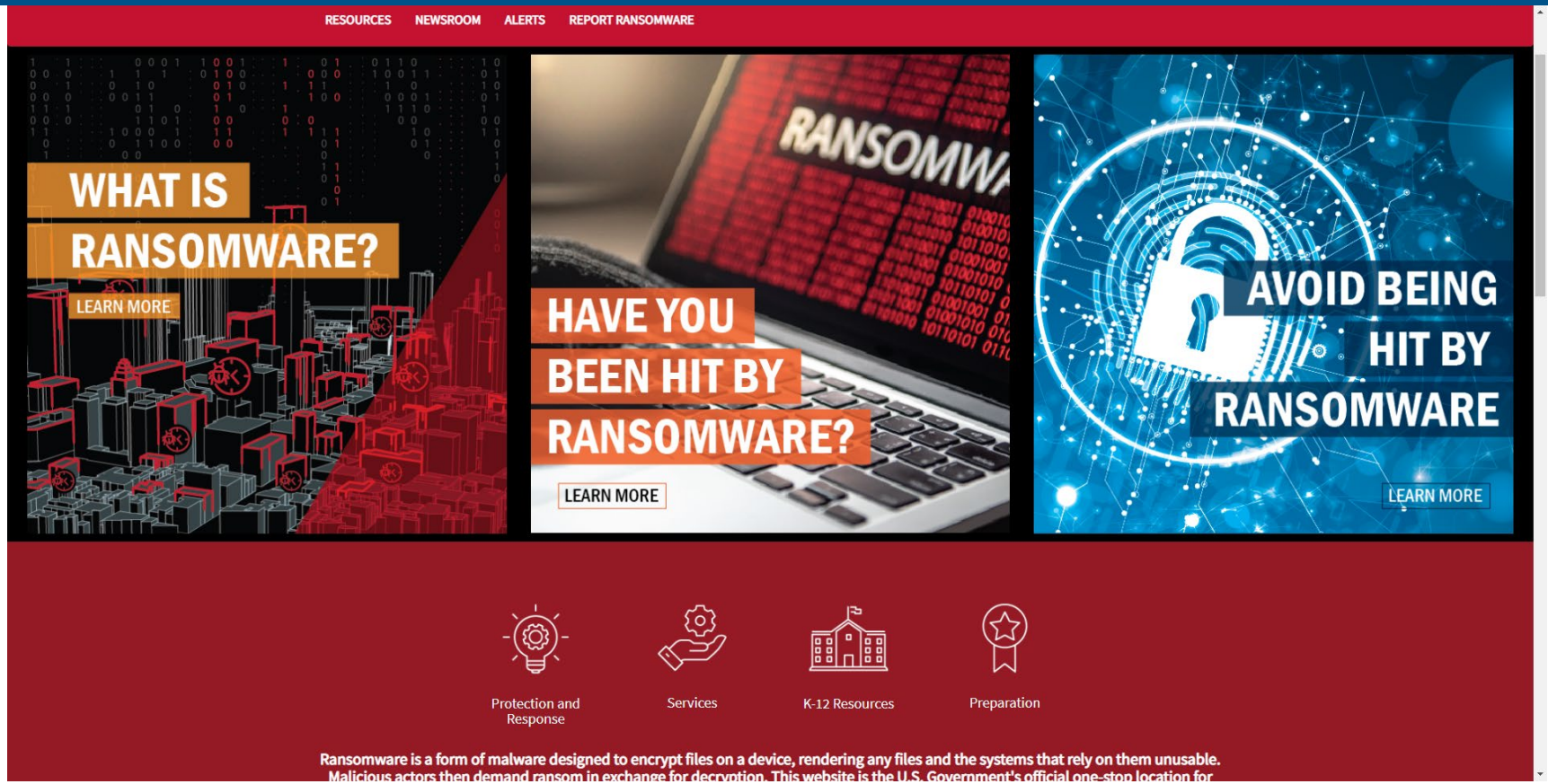
STOP. THINK. CONNECT. ™

Toolkit Materials for Different Audiences

- Students K-8, 9-12, and Undergraduate
- Parents and Educators
- Young Professionals
- Older Americans
- Government
- Industry
- Small Business
- Law Enforcement

https://www.cisa.gov/stopthinkconnect

StopRansomware.Gov



WWW.CISA.GOV or www.cisa.gov/stopransomware


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY