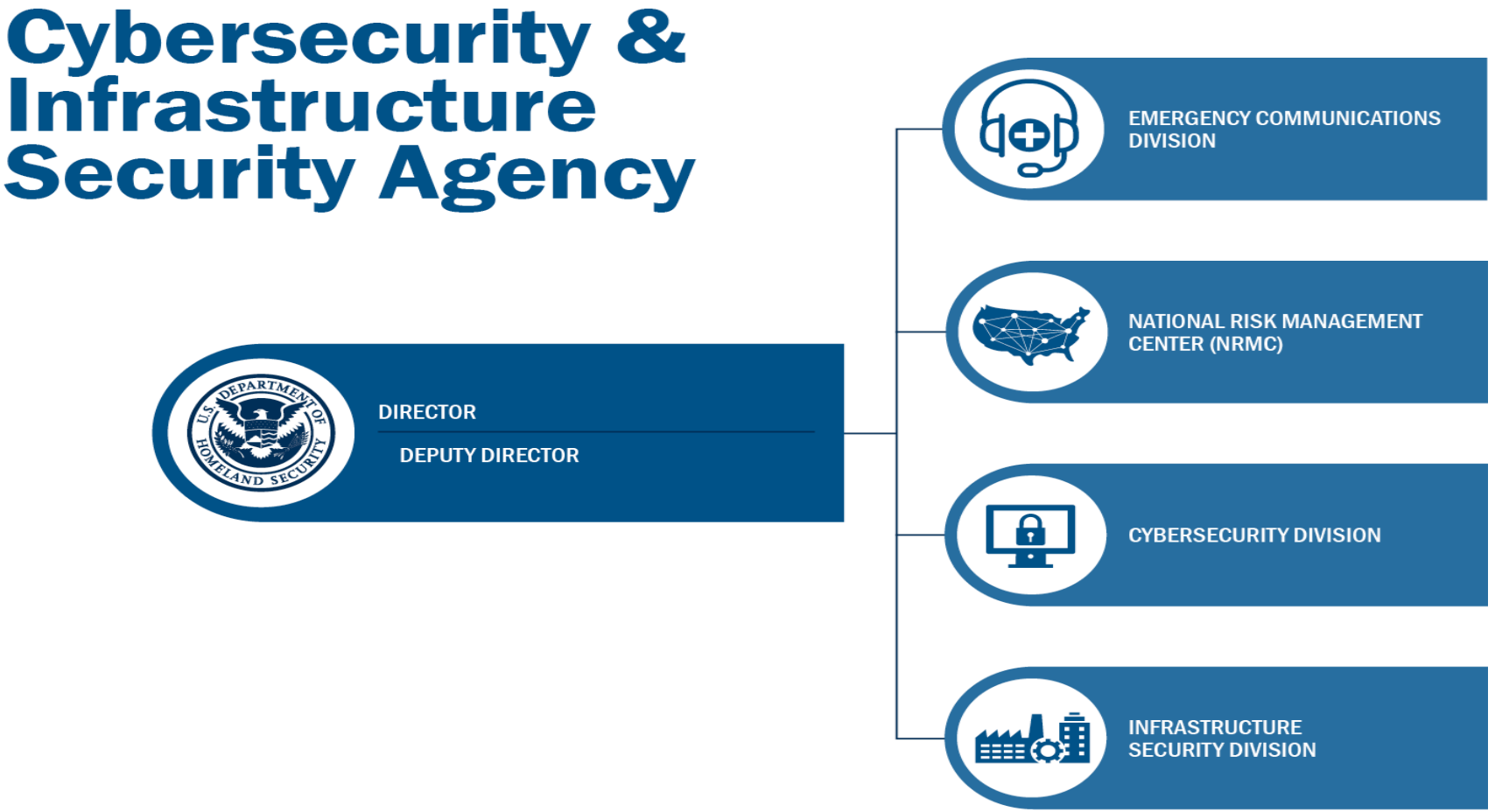
CISA OVERVIEW & SERVICES

SPACE CYBER SYMPOSIUM – ACCESS FOR START UPS
MAY 5, 2021

CISA Overview



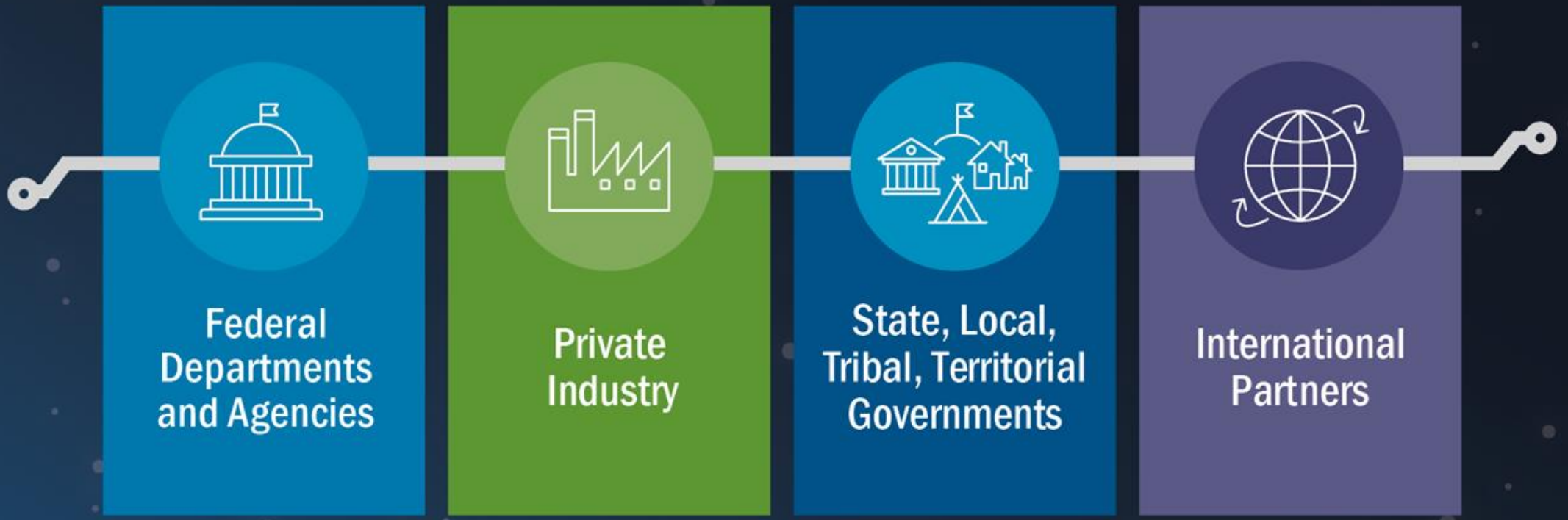
CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

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

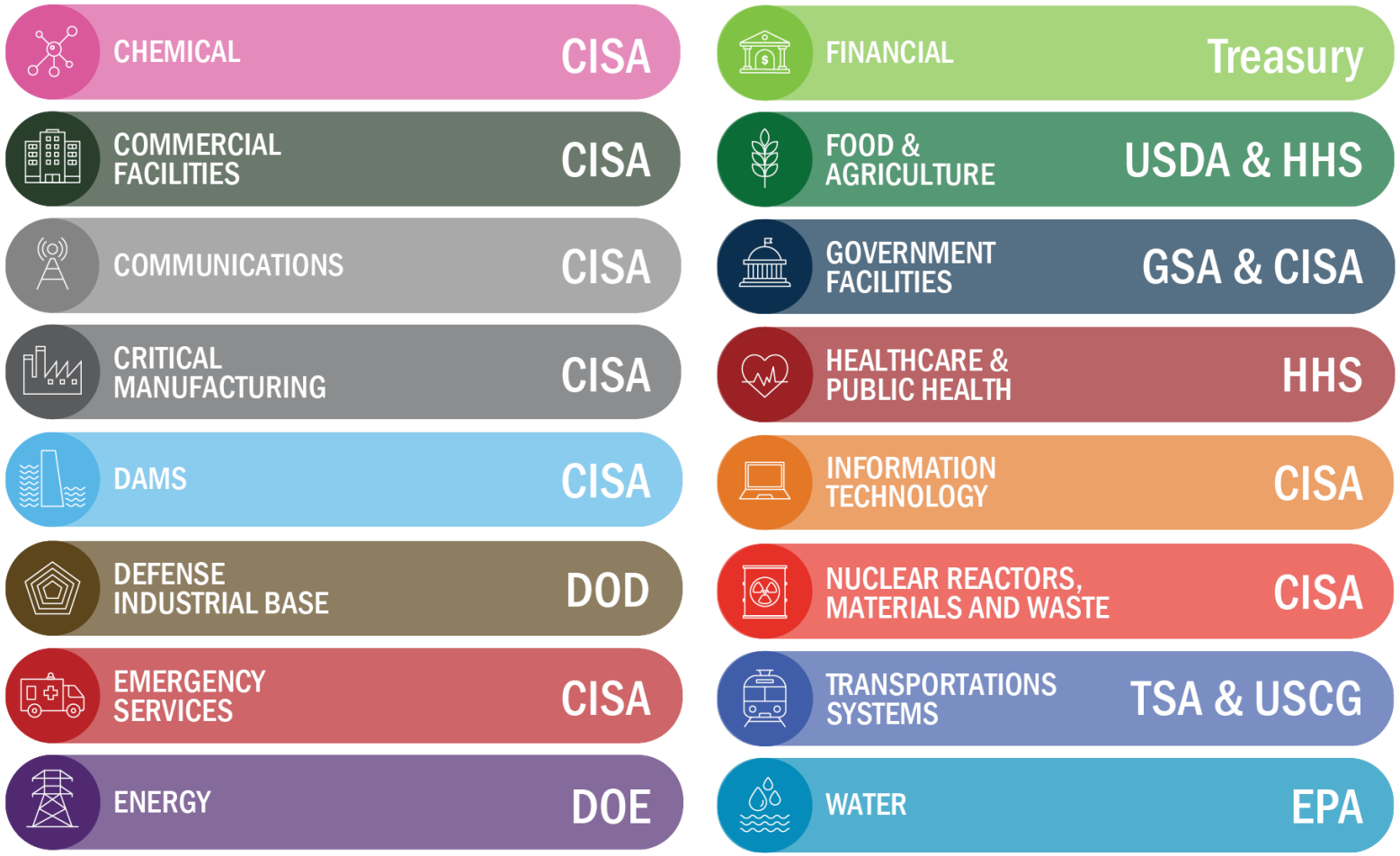
TLP:WHITE

WHO WE WORK WITH



20180904

16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies



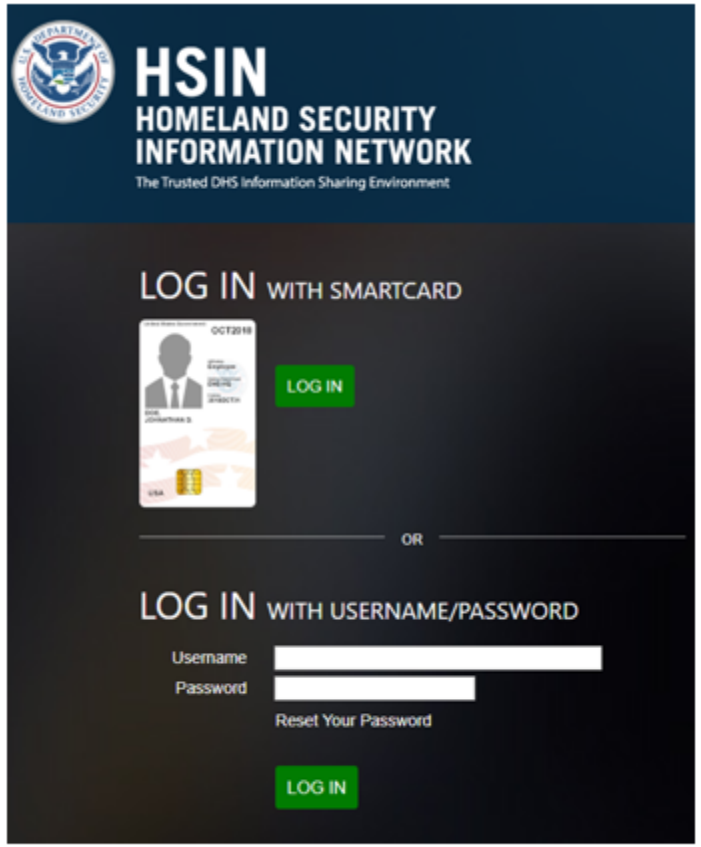
CISA's Gateway Service: Vulnerability Scanning

- Also known as Cyber Hygiene, offers persistent scanning of internet-accessible systems for vulnerabilities, configuration errors, and use of risky services.
- Conducts regular network and vulnerability scans and delivers a weekly report for action. Once initiated, this service is mostly automated and requires little direct interaction.
- For more information: vulnerability_info@cisa.dhs.gov

Other CISA Assessment Services

- **Phishing Campaign Assessment**: Measures your organization's propensity to click on email phishing lures. Results can be used to provide guidance for anti-phishing training and awareness.
- **Web Application Scanning**: Evaluates publicly-accessible websites for potential bugs and weak configurations and provides recommendations for mitigation.
- **Others**: Validated Architecture Design Review, Risk & Vulnerability Assessment, Critical Product Evaluation, etc.
- For all CISA assessments: https://www.cisa.gov/cyber-resource-hub

HSIN



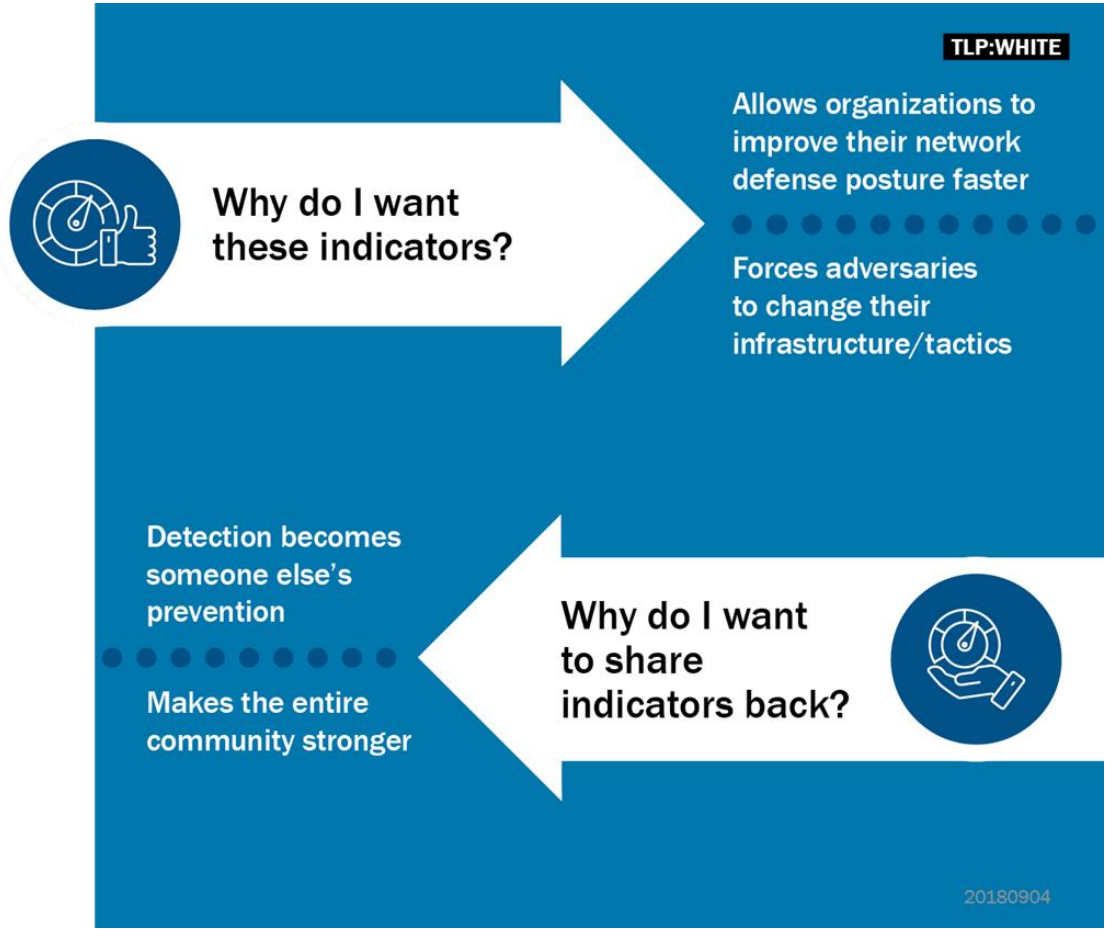
HSIN is the trusted network for homeland security mission operations to share Sensitive But Unclassified information. Capabilities include:

- Alerts and Notifications
- Document Repository
- Instant Messaging (HSIN Chat)
- Secure Messaging (HSINBox)
- Web Conferencing

AIS

AUTOMATED INDICATOR SHARING (AIS)

Enables exchange of cyber threat indicators at machine speed



ICS-JWG

- CISA hosts the Industrial Control Systems Joint Working Group (ICS-JWG) to partner across all sectors and private asset owners/operators, facilitate information sharing, and reduce risk to industrial control systems.
- Hosts bi-annual in-person meetings and webinars throughout the year.
- To become a member of the ICS-JWG, email the ICS-JWG Program Office at ICSJWG.Communications@hq.dhs.gov.

Other ICS Resources

- ICS-CERT Advisories provide timely information about current security issues, vulnerabilities, and exploits: https://us-cert.cisa.gov/ics/advisories
- CISA shares ICS security alerts, advisories, and reports through the National Cyber Awareness System (NCAS): https://us-cert.cisa.gov/ncas
- CISA offers several ICS-focused online training courses via the CISA Training Virtual Learning Portal (VLP): https://us-cert.cisa.gov/ics/Training-Available-Through-ICS-CERT

NCAS Alerts

- CISA's National Cyber Awareness System (NCAS) offers a variety of information for users with varied technical expertise. Those with more technical interest can read the cybersecurity Alerts, Analysis Reports, Current Activities, or Bulletins. Users looking for more general-interest pieces can read the Tips.
- **Current Activity**: Amplification of latest threats, vulnerabilities, and software patches
- **Bulletins**: Weekly summary on prioritized vulnerabilities
- **Activity Alerts**: Alerts on APT actors and malware campaigns
- **Analysis Reports**: Malware Analysis Reports (MARs) + IOCs
- A subscription to any or all of the NCAS products ensures that as soon as a product or alert is released by CISA, you will be the first to know. For more info: https://www.us-cert.gov/ncas

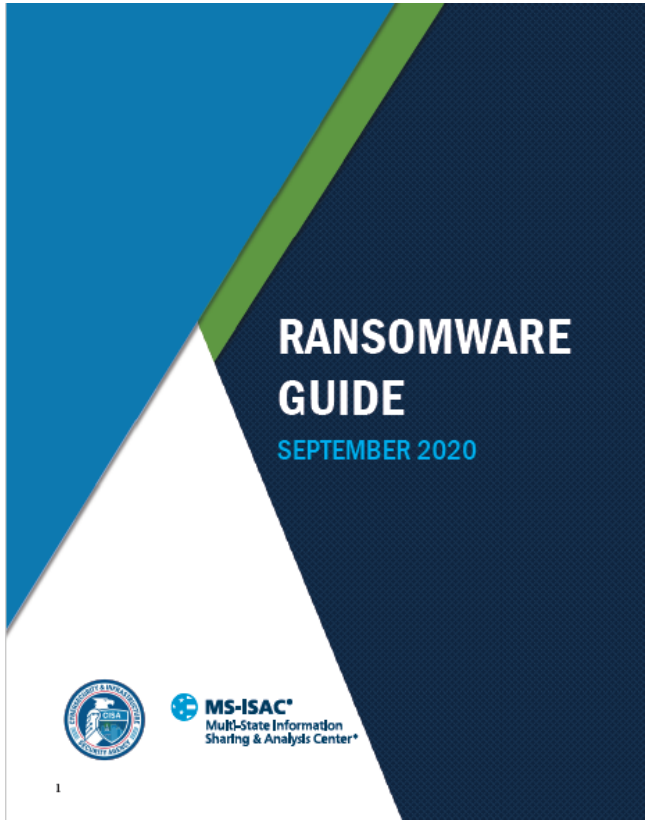
CISA Regional Security Advisors

- Protective Security Advisors (PSA) and Cybersecurity Advisors (CSAs) are regionally located and mapped to FEMA regions.
- The PSA program focuses on physical site security and resiliency assessments, incident management assistance, and vulnerability and consequence information.
- The CSA program offers cybersecurity assistance to CI owners and operators. CSAs provide cyber preparedness, assessments and protective resources, working group support and leadership, and incident coordination and support in times of cyber threat, disruption, and attack.
- For more information: https://www.cisa.gov/cisa-regions

Ransomware Guide

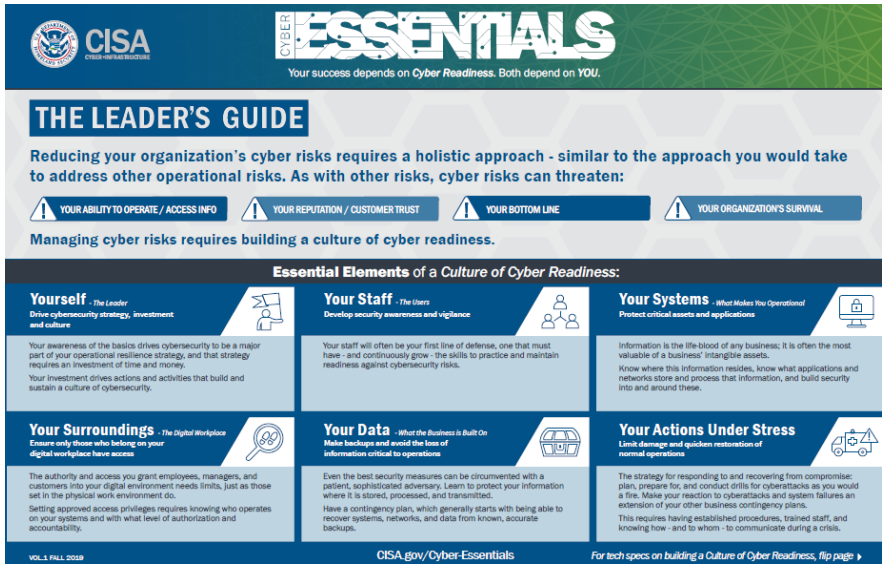
- On September 30, 2020, CISA and the Multi-State Information Sharing and Analysis Center released a joint Ransomware Guide, which is a customer centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack.

- Part 1: Ransomware Prevention Best Practices
- Part 2: Ransomware Response Checklist



Cyber Essentials Toolkit

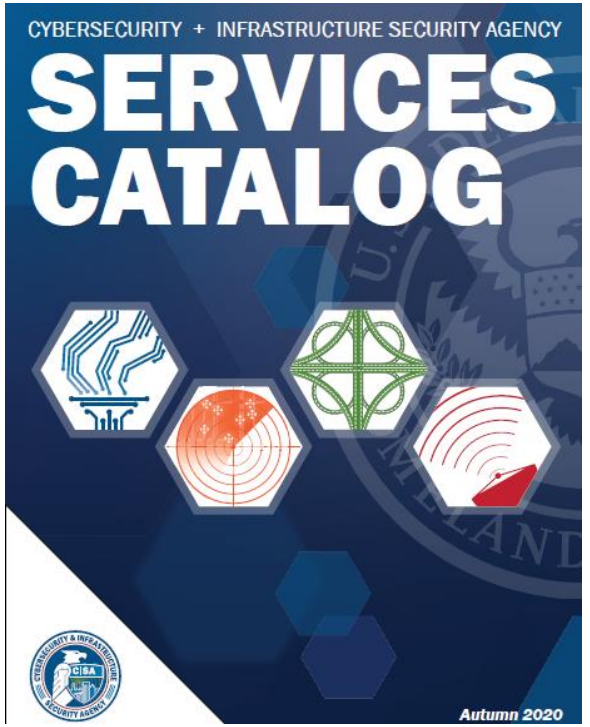
- CISA's Cyber Essentials is a guide for leaders of small businesses and small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.
- For a deeper look and greater insight, check out the Cyber Essentials Toolkits, a set of modules designed to break down the CISA Cyber Essentials into bite-sized actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential.



- Consistent with the NIST Cybersecurity Framework and other standards, the Cyber Essentials are the starting point to cyber readiness.

CISA Services Catalog

- The CISA Services Catalog is a single resource with information on services across all CISA mission areas that are available to federal and non-federal stakeholders.
- The Catalog is interactive, allowing users to filter and quickly select applicable services with just a few clicks. **Services available to industry partners start on pg. 22.**
- Periodically updated to keep up with the addition of new services.
- For questions about the services featured in the CISA Services Catalog, please email Central@cisa.gov.



Unclassified / TLP:WHITE