CYBERSECURITY PRESENTATION FOR THE TRANSPORTATION & PUBLIC WORKS SUBCOMMITTEE

MARCH 2023

Rahul Mittal
Cybersecurity Advisor– Region III
Cybersecurity and Infrastructure Security Agency

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

We lead the National effort to understand, manage, and reduce risk to our cyber and physical 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

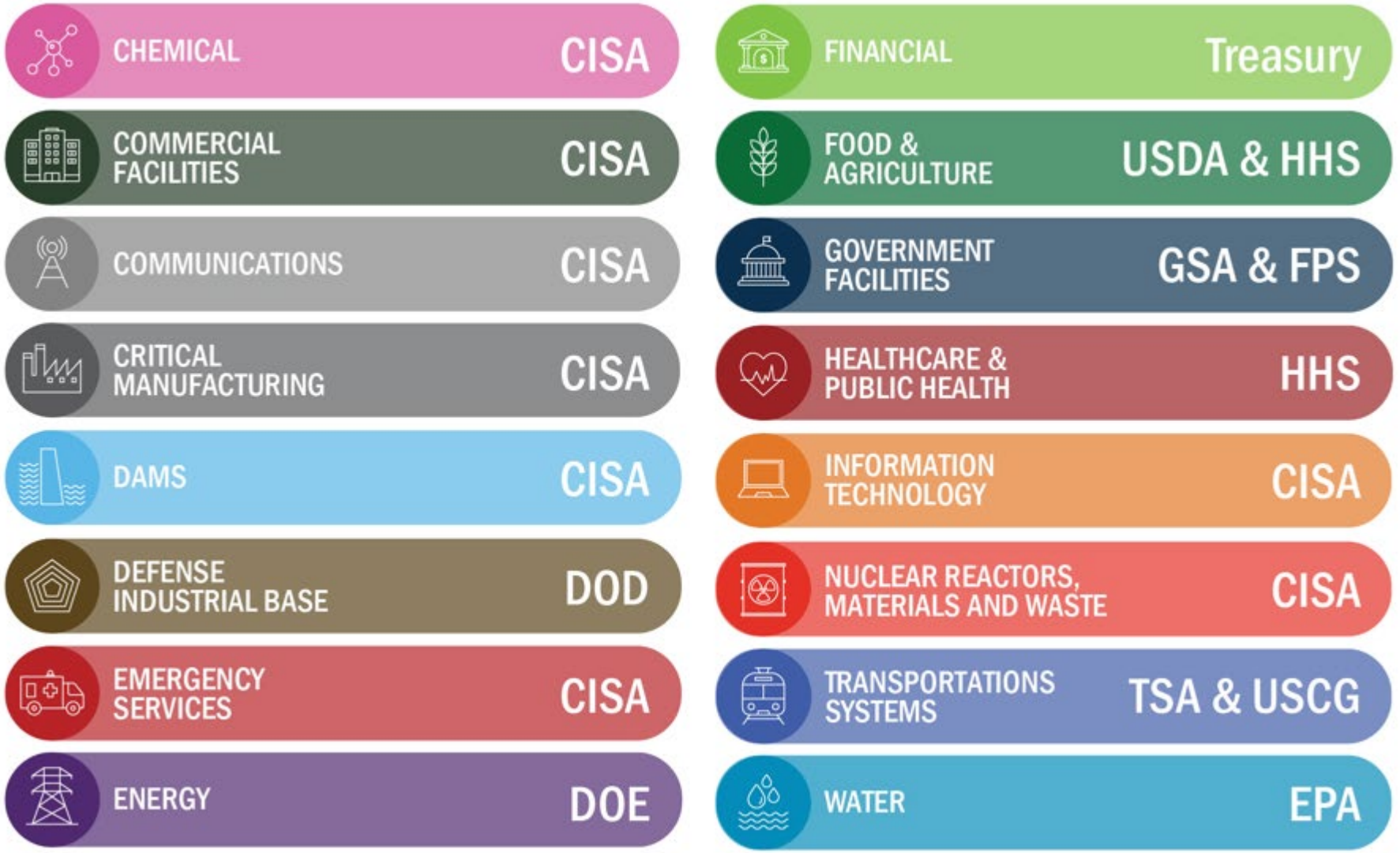
months | years | decades

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

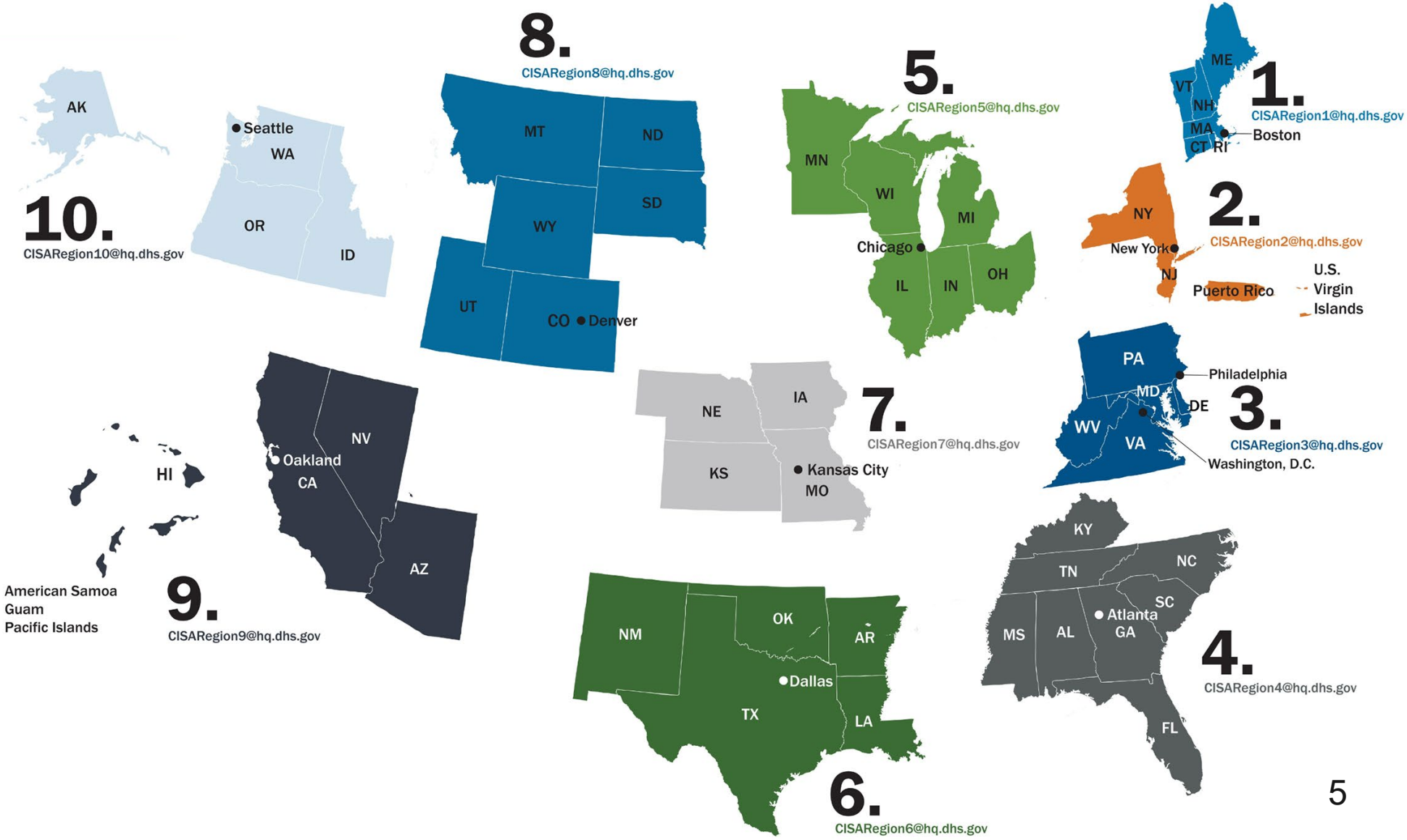
Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

16 Critical Infrastructure Sectors & SRMAs



CISA Regions

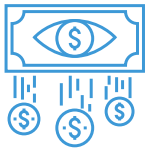


1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Irving, TX
7	Kansas City, MO
8	Lakewood, CO
9	Oakland, CA
10	Seattle, WA
CS	Pensacola, FL

Impacts of Cyber Attacks

Potential Future Impacts > Loss of Critical Data + Financial Loss + Damage to Reputation

Loss of Life



Loss of Revenue

Loss of Customer Trust

Loss of Intellectual Property

Legal Fines/Fees

Cyber Threats of Today

- **Ransomware (including RaaS)**
  - ESXIArg (VMWare ESXI servers)
  - Royal (ConnectWise)
  - Darkside (Market hacking tools stealing data)
  - REvil/ Sodinokibi (targeting MSPs)
  - Conti (LE, EM, SLTT), Lockbit, Clop, Egregor, Avaddon, Ryuk etc..

- **APTs and Nation-State Threats**
  - Killnet (Pro-Russian hackers conducting DDoS attacks)
  - APT28, APR29, APT41, etc.,
  - FIN7, FIN11, etc.

- **Other malware**
  - Remote Access Trojans (RATs)**: e.g., Trickbot**, **Emotet**, LokiBot, IcedID, BazarLoader
  - wiperware: NotPetya; Acid Rain, WhisperGate, Hermetic Wiper

- **Threats to External Dependencies**
  - 3rd party vendors, service providers, infrastructure providers
  - **Supply chain attacks**: SolarWinds, Kaseya, Kronos, etc.

- **Other Threats to Financial Services**
  - Phishing, BEC, PoS breach, Insider Threat, DDoS, etc.

Protective Measures in the “New Normal”

What your IT, and IT Security shops need to have in place (i.e., *the basics*)

Today

- Inventory all people, processes, technology and information
- Document critical systems and the services they support
- **Have a plan for responding to cyber incidents**
- **Backup all data and test backed-up data regularly**
- Deploy and update endpoint detection on all servers and workstations
- Turn on logging for all network appliances, servers and services
- **Develop and Implement comprehensive patch management process**

Tomorrow

- **Implement strong identity management practices (i.e., MFA)**
- **Plans to decommission End of Life systems**
- Develop and strengthen situational awareness
- Implement innovative security awareness training
- Implement a secure network architecture
- Conduct internal audits and periodic cyber assessments
- Utilize cyber attack frameworks when responding to cyber incidents

Protective Measures in the "New Normal"

Organizational Leaders

- **Know** business risks and treat cyber attacks as a risk area, to operations and to supply chains
- **Foster** a culture of operational resilience and cyber readiness
- **Incorporate** cybersecurity as a part of business strategy, including all external relationships
- **Build** and expand a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information, incident reporting, and response coordination

All End Users

- Participate in security awareness training and a general awareness in cyber threats
- Be aware of your digital footprint and know the end-user security features available to you
- Practice good operational security when participating in web conferencing
- Know the data backup options available and ensure locally stored data is backed up
- Be vigilant, accountable, and report incidents and suspicious activity immediately

Mechanics of a Cyber Attack

Who is the Target?

Staging Targets

- **Smaller organizations** with less sophisticated networks
- **Pre-existing relationships** with intended targets
- **Deliberately selected**, not targets of opportunity
- Examples: **vendors, integrators, suppliers,** and **strategic R&D partners**
- Used for **staging tools** and **capabilities**

Intended Targets

- **Small**, **medium**, and **large** organizations
- U.S. Targets focused across all sectors to include **Financial services sector**
- Sophisticated networks with more defensive cyber tools

CISA Offers No-Cost Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
    - Cyber Hygiene Services
    - Risk and Resilience-based Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - Remote Assistance
  - Incident Coordination
  - Threat intelligence and information sharing
  - Malware Analysis

- **Cybersecurity Advisors**
  - Incident response coordination
  - Cyber assessments
  - Workshops
  - Working group collaboration
  - Advisory assistance
  - Public Private Partnership Development

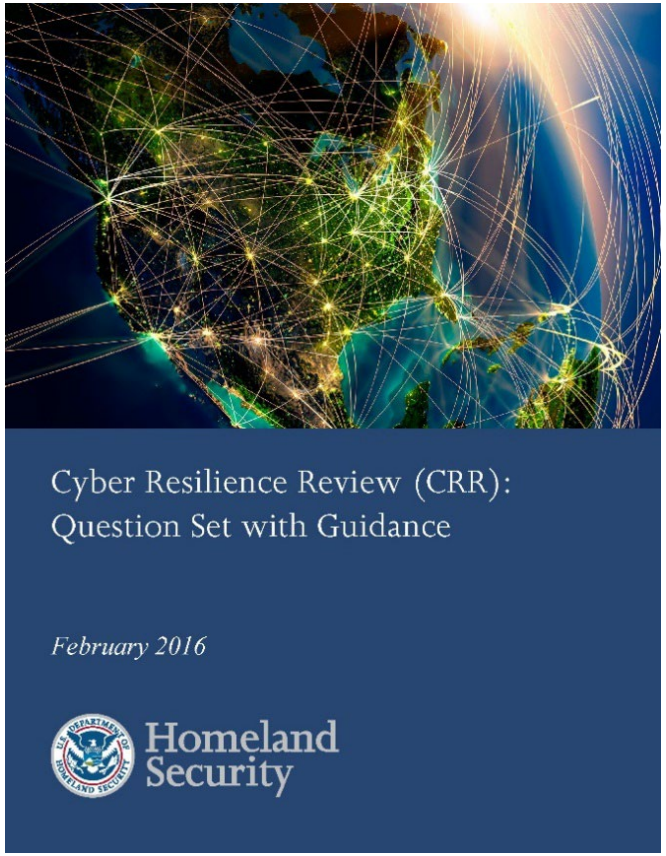
Contact CISA to report a cyber incident

Call 1-888-282-0870 | email report@cisa.dhs.gov | visit https://www.cisa.gov

Cyber Resilience Review

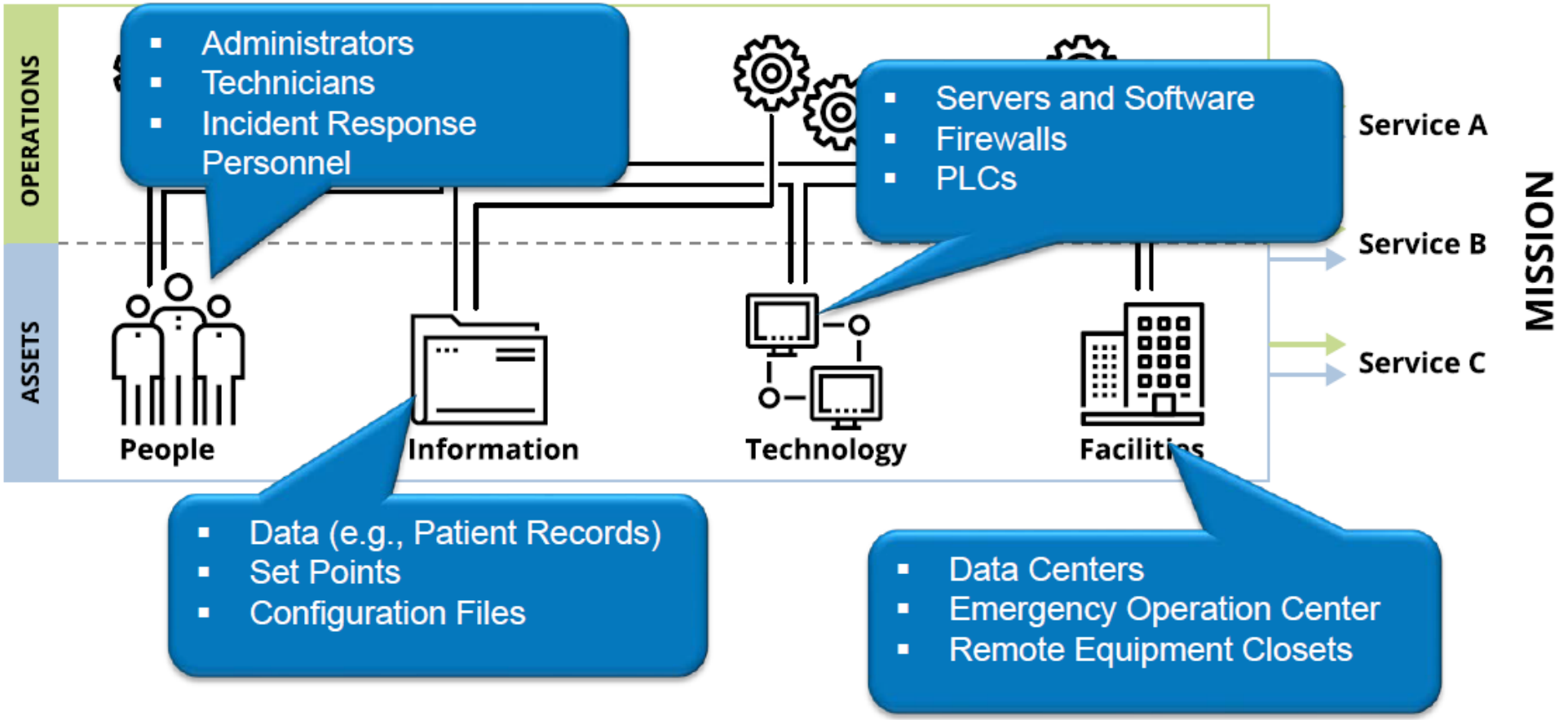
- **Purpose:** Evaluate operational resilience and cybersecurity practices of **critical services.**
- **Delivery:** Either CSA-facilitated, or self-administered
- **Benefits:** Report detailing an organizations capability and maturity in security management, and gaps against NIST CSF

Voluntary assessment *that is available at* ***no-cost*** *to requesting organizations*

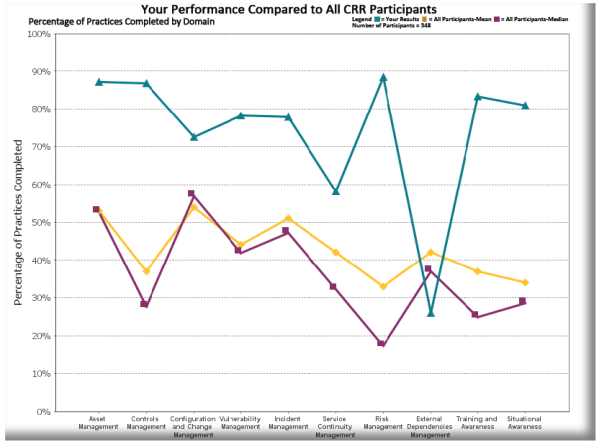


CRR Question Set & Guidance

Critical Service Assets and Examples



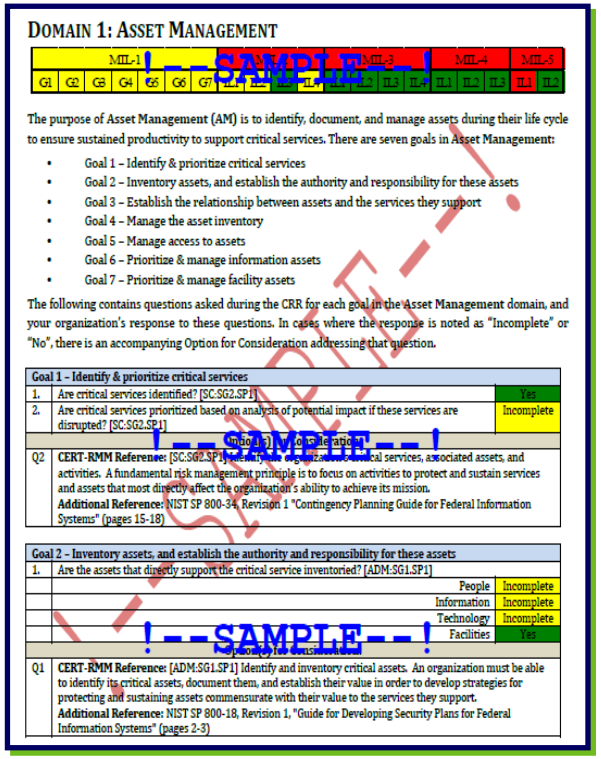
CRR Sample Report includes:



Comparison data with other CRR participants
**facilitated only*

A summary "snapshot" graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses



Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

Best Practices for Operational Resilience

- Know your assets being protected & their requirements, e.g., Confidentiality, Integrity, and Availability
  - Consider establishing an asset management process against its process description, standards, and procedures, and address non-compliance.
  - Consider documenting the Critical Services Asset Inventory to include the mapping of all devices and how they are connected.
  - Consider establishing an organization-wide approach to controls management that includes:
    - selecting from the organization's set of standard processes those processes that cover the controls management process and best meet the needs of the organizational unit or line of business
    - establishing the defined process by tailoring the selected processes according to the organization's tailoring guidelines
    - ensuring that the organization's process objectives are appropriately addressed in the defined process and ensure that process governance extends to the tailored processes
    - documenting the defined process and the records of the tailoring
    - revising the description of the defined process as necessary

Best Practices for Operational Resilience cont'd

- Manage asset configurations and changes
  - Consider sponsoring standards, and guidelines, including procedures, standards and guidelines for:
    - establishing and managing baseline configurations
    - change control
    - methods for measuring adherence to policy, exceptions granted, and policy violations
    - Manage changes to assets and to the asset inventory
- Know your vulnerabilities and manage those that pose the most risk
  - Consider establishing an organizational approach to vulnerability management that includes:
    - selecting from the organization's set of standard processes those processes that cover the vulnerability management process and best meet the needs of the organizational unit or line of business
    - establishing the defined process by tailoring the selected processes according to the organization's tailoring guidelines
    - ensuring that the organization's process objectives are appropriately addressed in the defined process and ensure that process governance extends to the tailored processes.
    - documenting the defined process and the records of the tailoring
    - revising the description of the defined process as necessary
  - Consider a Risk Acceptance process

Best Practices for Operational Resilience cont'd

- Be able to detect and respond to incidents
  - Consider measuring the performance of incident management activities to evaluate adherence to the process and share those results with higher-level management.
- Ensure workable plans are in place to manage disruptions
  - Development of COOP documents:
    - Establish requirements for recovery time objectives and recovery points
    - Develop and document asset requirements for Facilities supporting the critical service
    - Have a standard for testing service continuity. To include performing tests and reviewing those results to identify ways to improve.
- Know and address your biggest risks that considers cost and your risk tolerances
  - Consider establishing a IT Risk Management Process and the Business Risk process following a shared definition of risk.
    - identify risks that could prevent the delivery of the critical service.
    - Track identified risks to closure.
    - Document the process for performing risk management activities.
    - Develop and document a risk management process (adequate funding will be required)

Best Practices for Operational Resilience cont'd

- Ensure your people are trained on and aware of cybersecurity risks and practices
  - Insufficient processes to measure the effectiveness of training and awareness activities.
    - Consider acquiring training and awareness work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.

https://www.cisa.gov

https://www.cisa.govresources-tools/services?search_api_fulltext=cyber+resource+hub&sort_by=label

Filters

What are you looking for?

cyber resource hub

Sort by (optional)

Title

APPLY RESET

Topic +

Program +

Audience +

Task Type +

Readiness Level +

Services

RESPOND TO AN INCIDENT | FOUNDATIONAL, INTERMEDIATE, ADVANCED

Cyber Incident Response

For cybersecurity incidents that have a national security interest and align with national priorities, CISA provides incident response augmentation, artifact analysis, and coordination assistance.

ASSESS YOUR RISK LEVEL | INTERMEDIATE

Cyber Infrastructure Survey

The Cyber Infrastructure Survey provides a service-based view of the effectiveness of organizational security controls, cybersecurity preparedness, and the overall resilience of an organizationâ€™s cybersecurity ecosystem.

Cyber Resilience Review (CRR)

An assessment that evaluates an organization's operational resilience and cybersecurity practices.

ASSESS YOUR RISK LEVEL | FOUNDATIONAL

Cyber Security Assessment and Management (CSAM) Advisory Services

Ensure the CSAM application is effectively utilized and aligned with policy, posture, maturity, and culture.

Additional Information Sharing Opportunities

- **Multi-State Information Sharing and Analysis Center:**
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC™

ONG-ISAC

National Defense ISAC

- **ISACs and ISAOs:**
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to m ore info AC visit www.nationa more on ISAOs visit www.isao.c t.

RETAIL & HOSPITALITY ISAC

Real Estate ISAC Information Sharing and Analysis Center
Serving the Commercial Facilities Sector

WATER ISAC

SPACE ISAC

DNG-ISAC

H-ISAC HEALTH - ISAC

REN-ISAC

MEISAC MEDIA + ENTERTAINMENT INFORMATION SHARING ANALYSIS CENTER

FS-ISAC

IT ISAC

E-ISAC

AUTO-ISAC Automotive Information Sharing and Analysis Center

AVIATION ISAC

Cyber Hygiene Services

A persistent scanning service of internet-accessible systems for vulnerabilities, configuration errors and suboptimal security practices.

Email vulnerability @ cisa.dhs.gov and attach a copy of:

- Service Request Form (SRF)
- Cyber Hygiene Acceptance letter.

Sample reports can be found on the Vulnerability Management webpage at: https://us-cert.cisa.gov/resources/ncats

Additional CISA Resources:

- **STOP RANSOMWARE:** https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr
- **Download the CSET Tool:** https://www.cisa.gov/downloading-and-installing-cset
- **Cyber Hygiene Services:** email us at vulnerability@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services” to get started.
- **Cyber Resource Hub:** https://www.cisa.gov/cyber-resource-hub
- **Cyber Essentials:** https://www.cisa.gov/cyber-essentials
- **Vulnerability Disclosure Policy Template:** https://www.cisa.gov/vulnerability-disclosure-policy-template
- **CISA Incident Reporting Form:** https://us-cert.cisa.gov/forms/report
- **Cybersecurity Training and Exercises:** https://www.cisa.gov/cybersecurity-training-exercises
- **CISA Tabletop Exercise Packages:** https://www.cisa.gov/cisa-tabletop-exercises-packagesCISA
- **Know Exploited Vulnérabilités (KEV) Catalog:** https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **Cyber Incident Response : https://us-cert.cisa.gov/forms/report and/or Filing a Complaint with IC3:** https://www.ic3.gov/

Rahul Mittal
Cybersecurity Advisor, Region 3
National Capitol Region
Rahul.mittal@cisa.dhs.gov

Regional Support:
CISARegion3@hq.dhs.gov

To Report an Incident:
https://us-cert.cisa.gov/report

Media Inquiries:
CISAMedia@cisa.dhs.gov

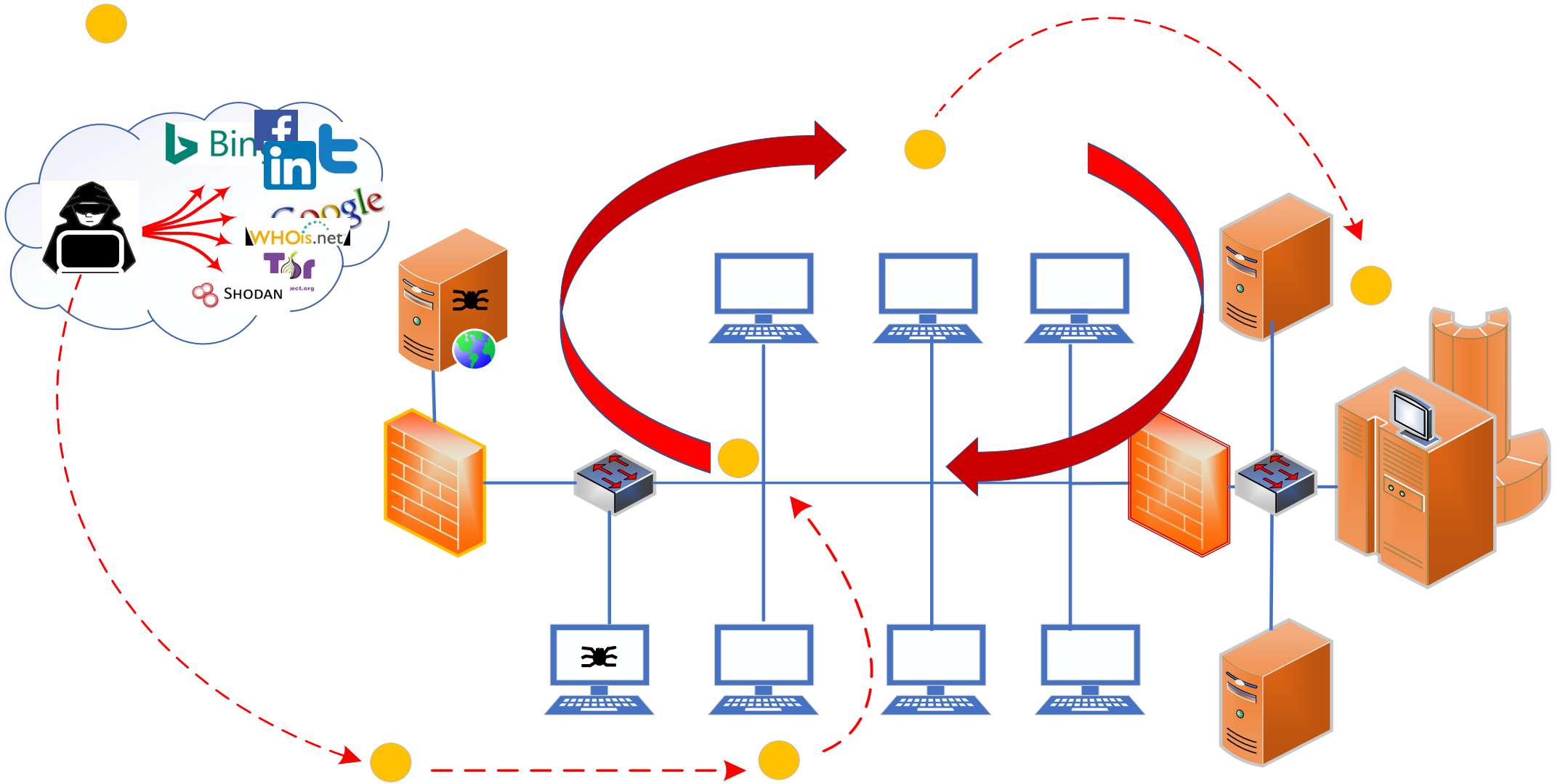

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Cyber Resilience Review Domains

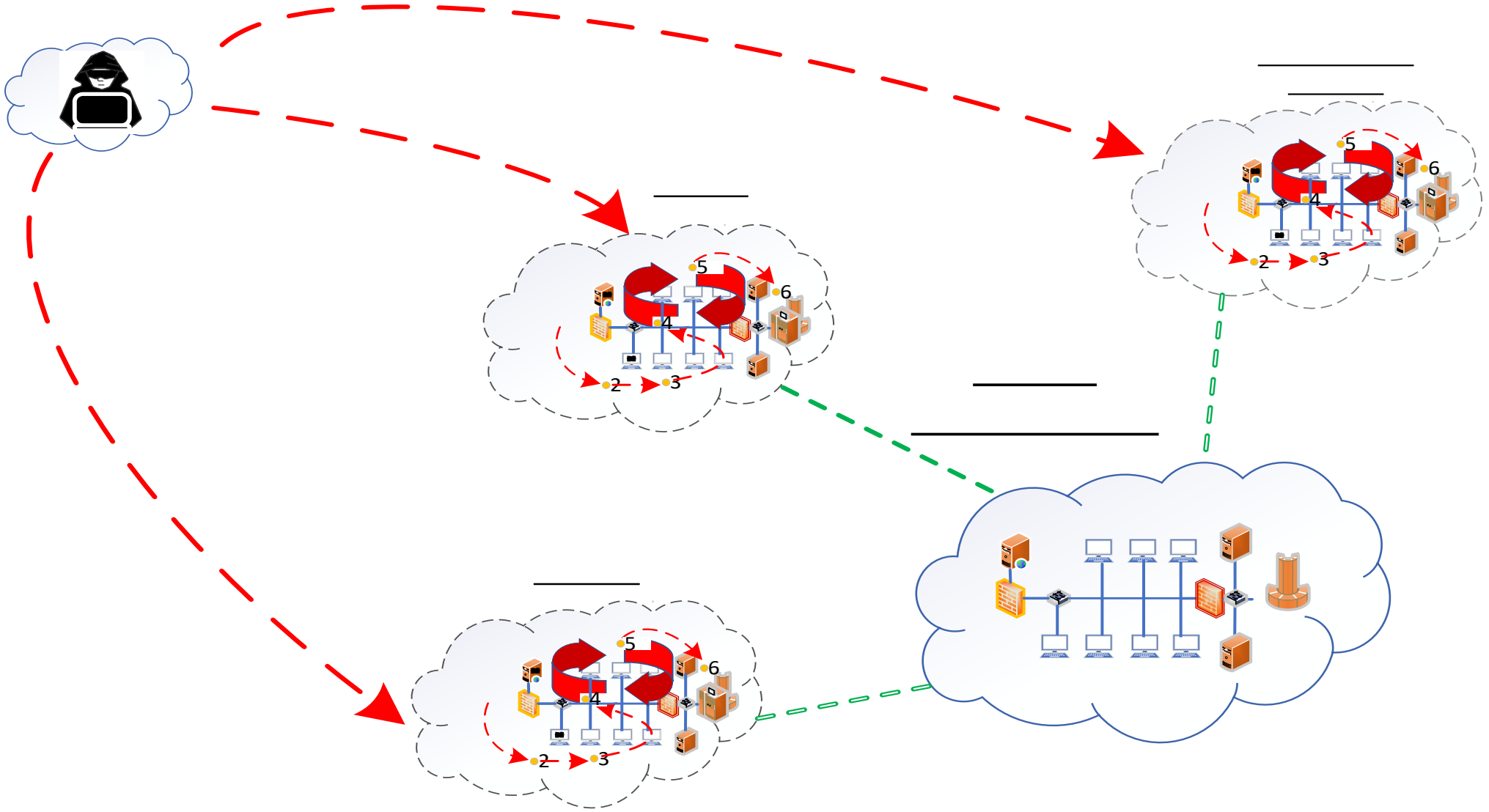
Asset Management Know your assets being protected & their requirements, e.g., Confidentiality, Integrity, and Availability	**Risk Management** Know and address your biggest risks that considers cost and your risk tolerances
Configuration and Change Management Manage asset configurations and changes	**Service Continuity Management** Ensure workable plans are in place to manage disruptions
Controls Management Manage and monitor controls to ensure they are meeting your objectives	**Situational Awareness** Discover and analyze information related to immediate operational stability and security
External Dependencies Management Know your most important external entities and manage the risks posed to essential services	**Training and Awareness** Ensure your people are trained on and aware of cybersecurity risks and practices
Incident Management Be able to detect and respond to incidents	**Vulnerability Management** Know your vulnerabilities and manage those that pose the most risk

For more information: https://www.cisa.gov/cyber-resource-hub

Mechanics of a Cyber Attack - 1



Mechanics of a Cyber Attack - 2



Cyber Statistics

SOBERING CYBER STATS

1 IN 3 HOMES
with computers are infected with
MALICIOUS SOFTWARE

65% OF AMERICANS
who went online received
at least one online scam offer.

Worldwide, consumers
LOST $358
+21 HOURS
on average per year
dealing with online crime.

47% OF AMERICAN ADULTS
have had their personal information
exposed by cyber criminals.

600,000 ACCOUNTS HACKED
every single day.

THE #1 CYBER CRIME is the
IMPOSTER SCAM
with 1 in 5 people reporting
a financial loss.