Ron Ford
Cyber Security Advisor, New England (Region 1)
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

CISA's ROLE

Cyber Threat Landscape

Cybersecurity and Resilience

CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

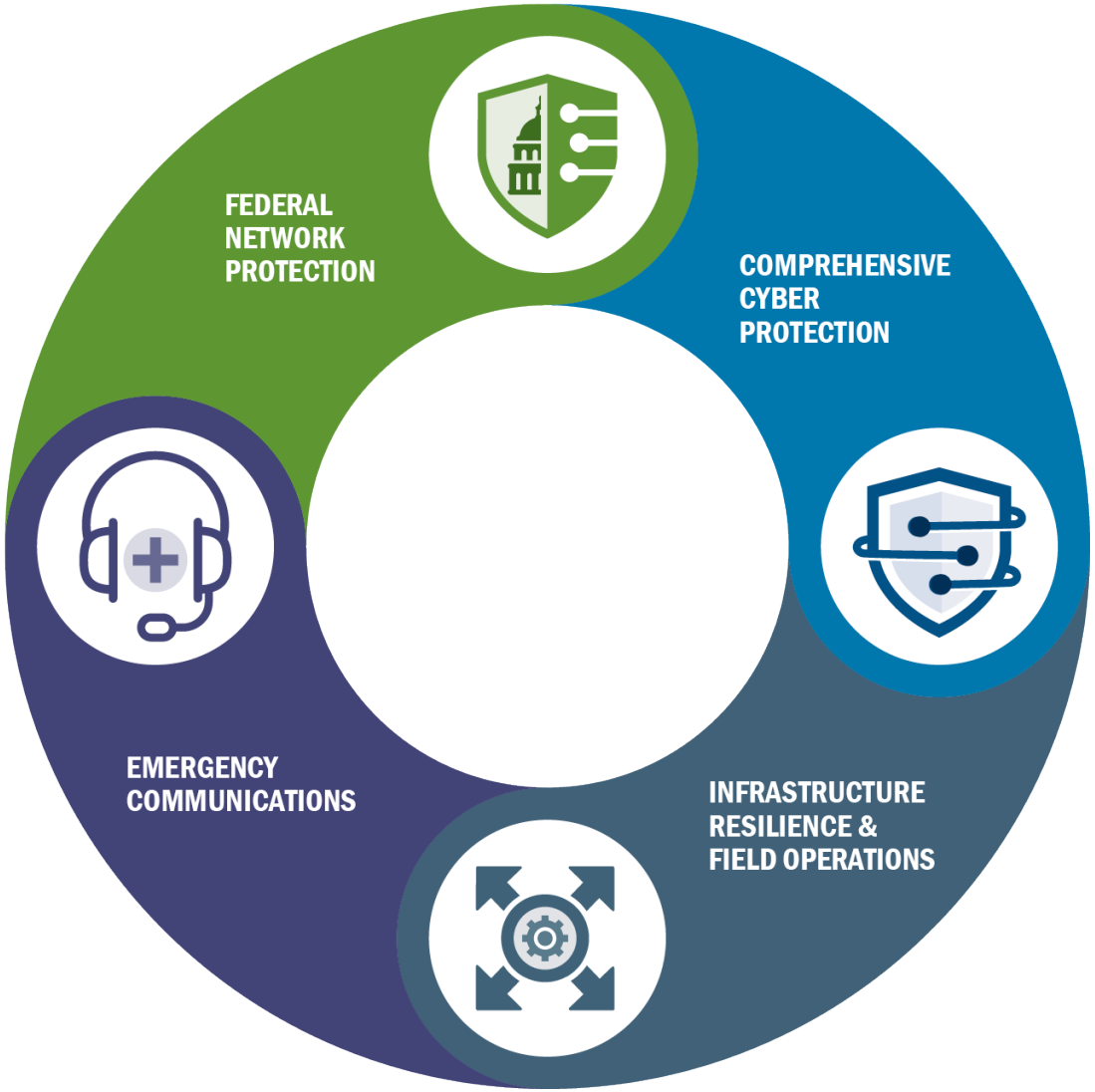
Secure and resilient infrastructure for the American people.

MISSION

Lead the Nation's efforts to understand and manage risk to our critical infrastructure.

We are the Nation's Risk Advisors

CISA leads national risk management for cyber and physical infrastructure



Today's Risk Landscape

America remains at risk from a variety of threats:

INSIDER THREAT

ACTS OF TERRORISM

CYBER ATTACKS

EXTREME WEATHER

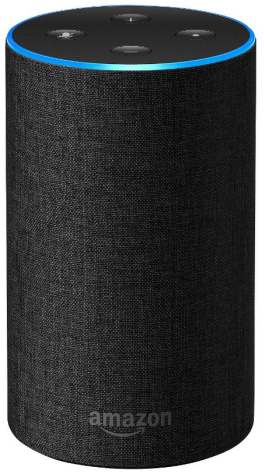
PANDEMICS

ACCIDENTS OR TECHNICAL FAILURES

CYBER THREAT LANDSCAPE

6

Ever Expanding Attack Surface



CISA
CYBER+INFRASTRUCTURE

Most Common Cyber Threats

- **RANSOMWARE**
- **PHISHING CAMPAIGNS**
- **Business E-mail Compromise**
- **Lack of Software Patching**
- **WEAK PASSWORDS**
- **Misconfiguration of Technology**
- **Supply Chain (Hardware, Software, Cloud Services)**

***All listed will increase the likelihood of a compromise or service disruption.**

CISA
CYBER+INFRASTRUCTURE

Cybersecurity Risks ARE Business Risks

- Technology affords access to more data to make informed decisions
- Technology introduces new risk to data
- Technology risks should be considered a business risk
  - Availability of data
  - Integrity of data
  - Confidentiality of data

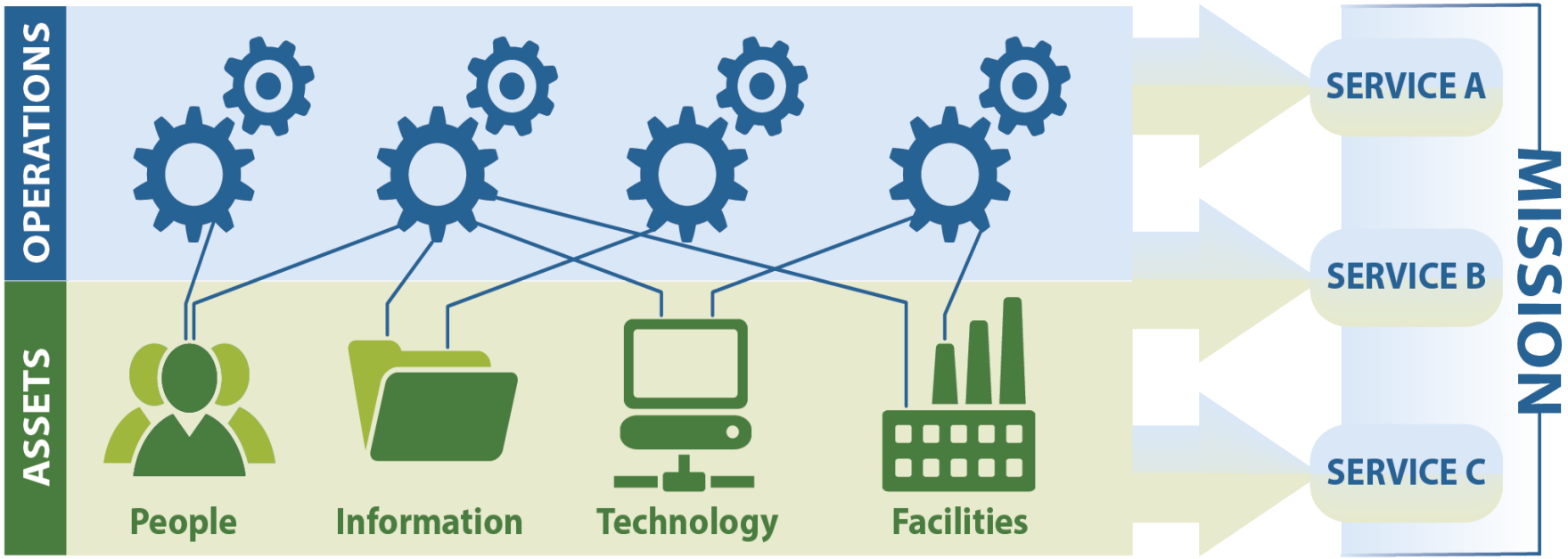
CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY & RESILIENCE

11

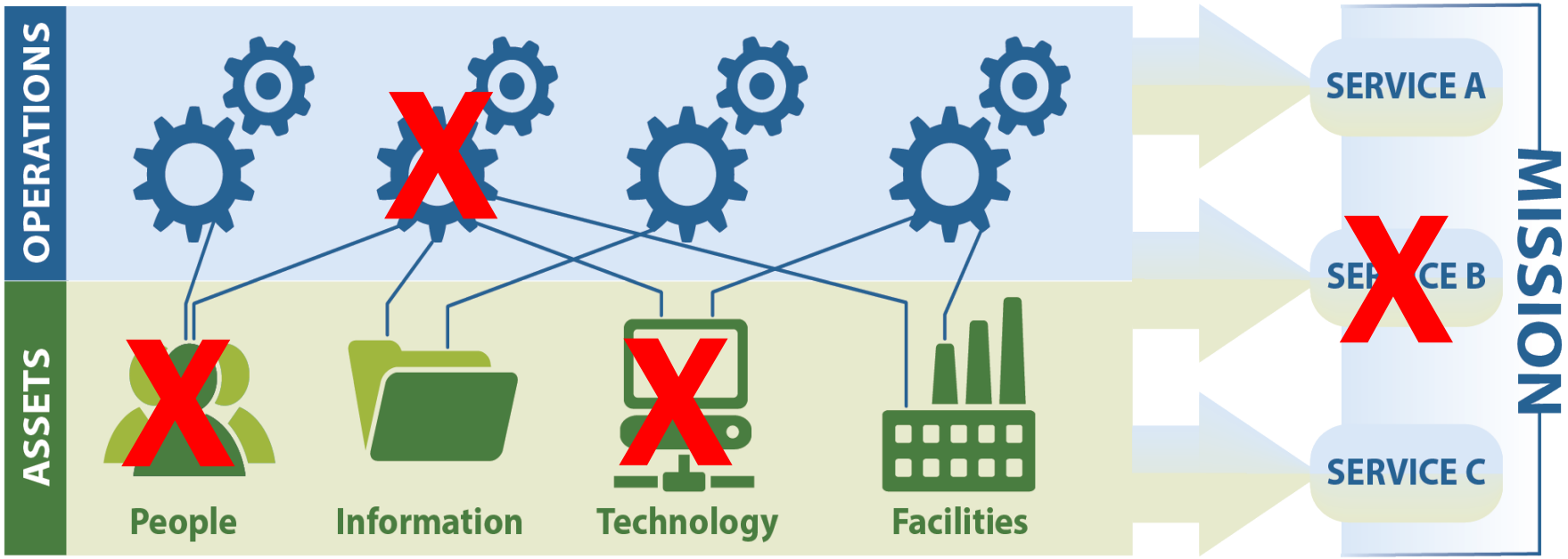
Critical Service Focus

Organizations use assets (people, information, technology, and facilities) to provide operational services and accomplish missions.



Critical Service Focus

Disruptions will occur. The organization should determine service priority and associated risks to the mission.



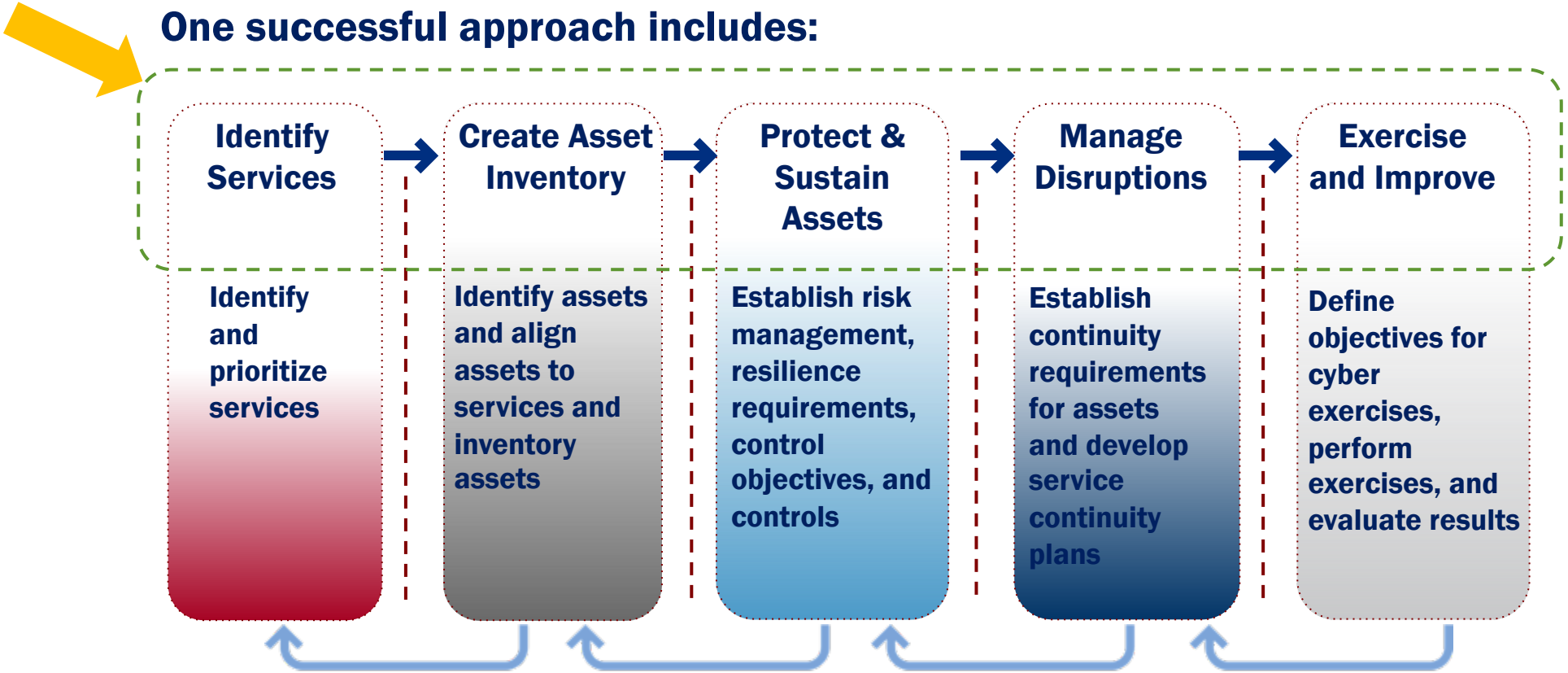
Resilience Emerges From What You Do

- Consider your health.
  - How do you become healthy?
  - Can you buy good health?
  - Can you "manufacture" good health?
- You can't buy it in a product.
- *Good health* and *resilience* are both emergent properties.
- They develop – or emerge – from what we do.

CISA
CYBER+INFRASTRUCTURE

Working toward Cyber Resilience

Follow a framework or general approach to cyber resilience.
One successful approach includes:



CISA
CYBER+INFRASTRUCTURE

CISA Insights on COVID-19

- **Risk Management for Novel Coronavirus (COVID-19)**

- **This product is for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread from of COVID-19.**

- **What's in this guide:**
  - **Actions for Infrastructure Protection**
  - **Actions for your Supply Chain**
  - **Cybersecurity for Organizations**
  - **Cybersecurity Actions for your Workforce and Consumers**

- **To stay current with CISA's efforts regarding the COVID-19, visit: cisa.gov/coronavirus.**

CISA
CYBER+INFRASTRUCTURE

CISA Cyber Essentials

- **CISA Services Catalog:**
  - **https://www.cisa.gov/publication/cisa-services-catalog**
- **Cyber Essentials Toolkit:**
  - **https://www.cisa.gov/cyber-essentials**
- **National Cyber Security Alliance:**
  - **https://www. staysafeonline.org**

Securing Industrial Control Systems

- **July 8, 2020: CISA released "Securing Industrial Control Systems: A Unified Initiative"**

- **This five-year strategy provides a framework and guidance to strengthen and unify industrial control systems (ICS) cybersecurity to better protect the essential services provided daily to Americans**

CISA
CYBER+INFRASTRUCTURE

Securing Industrial Control Systems

- The initiative builds around four crosscutting pillars:
  - Pillar 1: Ask more of the ICS Community, deliver more to them.
  - Pillar 2: Develop and utilize technology to mature collective ICS cyber defense.
  - Pillar 3: Build “deep data” capabilities to analyze and deliver information that the ICS community can use to disrupt the ICS cyber kill chain.
  - Pillar 4: Enable informed and proactive security investments by understanding and anticipating ICS risk.

CISA
CYBER+INFRASTRUCTURE

CISA Cybersecurity Services

22

Criticality of Periodic Assessments

- **Periodic assessments are essential for resilience, helping you:**
  - **Measure your cybersecurity efforts**
  - **Manage improvements over time**

Cybersecurity Advisor Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

In support of that mission, Cybersecurity Advisors (CSAs):

- **Assess: Evaluate critical infrastructure cyber risk.**
- **Promote: Encourage best practices and risk mitigation strategies.**
- **Build: Initiate, develop capacity, and support cyber communities-of-interest and working groups.**
- **Educate: Inform and raise awareness.**
- **Listen: Collect stakeholder requirements.**
- **Coordinate: Bring together incident support and lessons learned.**

CISA CYBER+INFRASTRUCTURE

CSA Deployed Personnel

Contact cyberadvisor@cisa.dhs.gov

CISA
CYBER+INFRASTRUCTURE

Sampling of Cybersecurity Offerings (Voluntary & No-Cost)

Preparedness Assistance:

- Cybersecurity Advisors
  - Advisory Services
  - Assessments
  - Working group collaboration
  - Best Practices
  - Incident assistance coordination
- Protective Security Advisors
  - Assessments
  - Incident liaisons between government and private sector
  - Support for National Special Security Events

CISA
CYBER+INFRASTRUCTURE

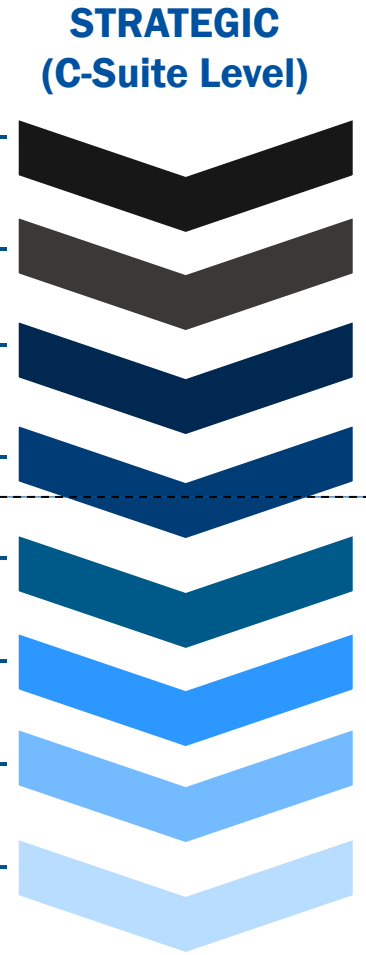
Range of Cybersecurity Assessments (Voluntary & No-Cost to You)

Strategic

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool (Strategic/Technical)

Technical

- Phishing Campaign Assessment (EVERYONE)
- Vulnerability Scanning / Hygiene (Technical)
- Validated Architecture Design Review (Technical)
- Risk and Vulnerability Assessment (Technical)



CISA
CYBER+INFRASTRUCTURE

BEST PRACTICES

MAKE YOUR OWN LUCK!

- Leadership Must OWN the Issue
- Be Prepared – EXERCISE
- Good Cyber Hygiene – Blocking and Tackling
- Defend and Continue to Operate
- Risk Management – What Can I Accept?
  - + Balance Security, Mission and Privacy
- Leverage Relationships

CISA
CYBER+INFRASTRUCTURE

QUESTIONS?

Contact Us

Ron Ford
DHS/CISA Cybersecurity Advisor
Region 1 - New England
Ron.Ford@cisa.dhs.gov
cyberadvisor@cisa.dhs.gov
https://www.cisa.gov/csa
www.cisa.gov/cybersecurity

Report Incidents:

DHS/CISA

24/7 Line: 888-282-0870

Central@cisa.gov

https://www.cisa.gov

CISA
CYBER+INFRASTRUCTURE

CISA

CYBER+INFRASTRUCTURE