CYBERSECURITY FRAMEWORK 101

RSA

The NIST Cybersecurity Framework (CSF) is the Federal government's high-profile program to help private organizations in their cybersecurity strategies. The CSF addresses standards, guidelines, and best practices to promote the protection of information and information systems.

GOAL

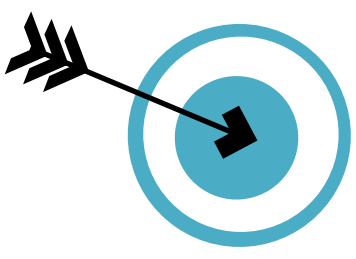
THE CSF IS FOCUSED ON SECURING AMERICA'S CRITICAL INFRASTRUCTURE

KICKED-OFF BY EXECUTIVE ORDER

E.O. 13636 SIGNED ON 2/19/13, CALLS FOR A NATIONAL CYBERSECURITY FRAMEWORK.

MAJOR BREACHES

The EO was a response to threats of growing frequency and intensity, and over-the-horizon considerations.



1/31/13 to 2/7/13: 6 major cyber incidents received around-the-clock coverage – just days before the State of the Union address.

MISSION OF THE EO AND CSF

- Risk-based critical infrastructure methodologies, developed in public-private partnership.
- NIST to develop standards for critical infrastructure framework metrics
- Develop common taxonomy and mechanisms to describe state of Cyber readiness & identify areas for improvement
- Identify national/regional critical infrastructure cyber footprint
- Improve information sharing on threat intelligence

BECOMING A DE FACTO REQUIREMENT

SEC is starting to gauge compliance with the CSF for certain organizations in their jurisdiction.

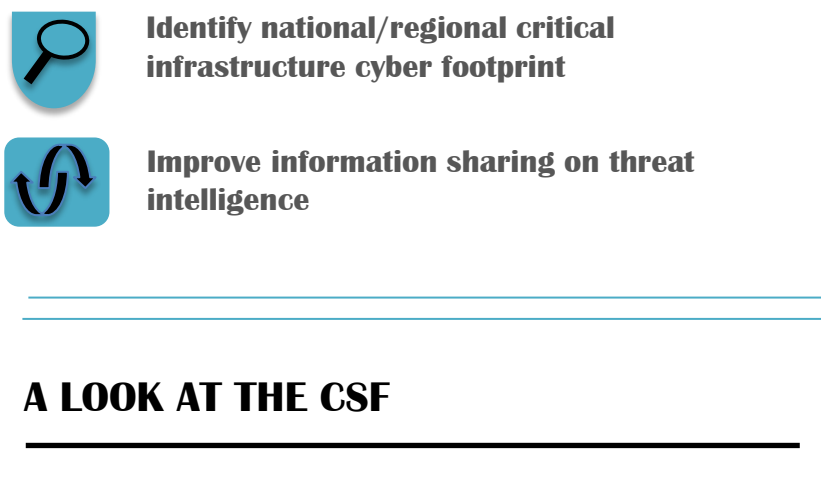
HHS considering whether contractors should be required to have Cyber Insurance.

A LOOK AT THE CSF

16 CRITICAL INFRASTRUCTURE SECTORS

- Information Technology
- Critical Manufacturing
- Commercial Facilities
- Government Facilities
- Food & Agriculture
- Communications
- Defense Industrial Base
- Banking & Financial Services
- Dams
- Nuclear Industry
- Emergency Services
- Water & Wastewater
- Energy
- Chemical
- Transportation Systems
- Healthcare & Public Health

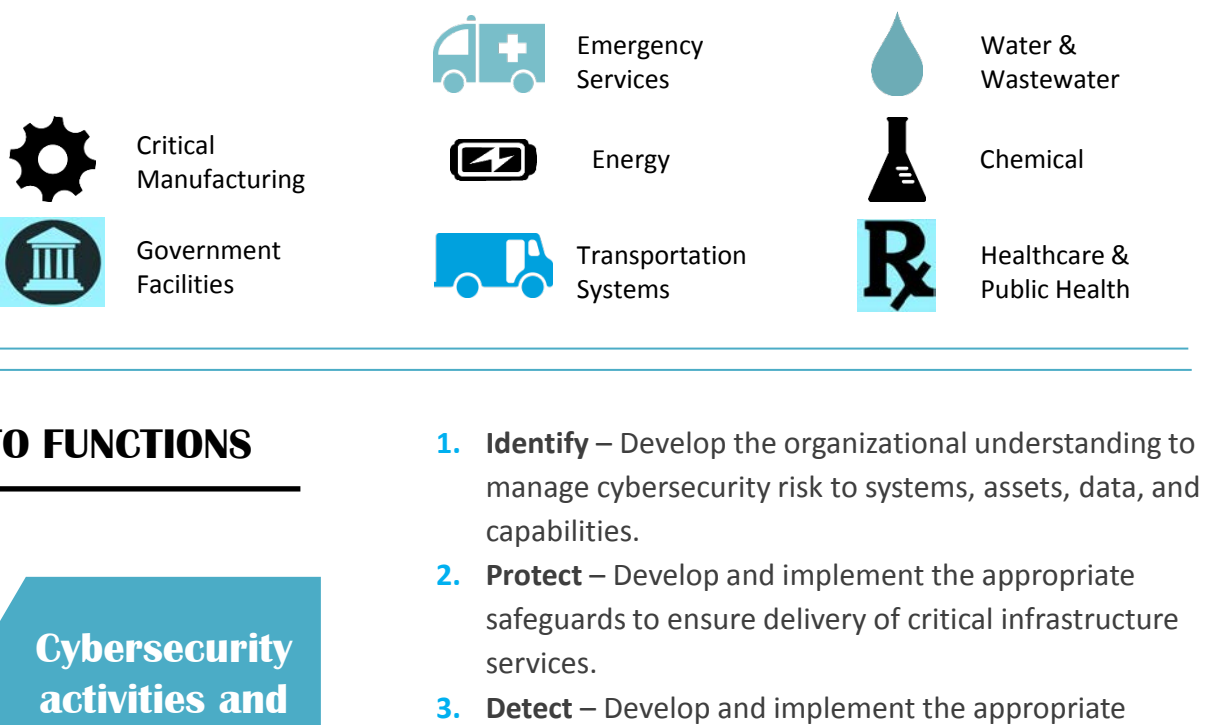
THE CSF IS GROUPED INTO FUNCTIONS



1. **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3. **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
4. **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5. **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

RSA Net Defender OPERATIONALIZING THE CSF

RSA's Advanced Cyber Defense (ACD) team offers the Net Defender program to strategize, implement and operate outcome-based security capabilities aligned to the CSF – built for the specific needs and environments for your business.



RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA gives customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime.

For more information about RSA, please go to www.rsa.com.

RSA