C3 VOLUNTARY PROGRAM

WELCOME TO THE COMMUNITY.

#ccubedvp

C³ VOLUNTARY PROGRAM OVERVIEW

Directives in Executive Order 13636:

- The National Institute of Standards and Technology (NIST) should develop a Cybersecurity Framework
  (the Framework) for reducing cyber risks to critical infrastructure

- A voluntary program for critical infrastructure cybersecurity should promote use of the Framework: Critical Infrastructure Cyber Community (C³) Voluntary Program

"Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity."

- White House Executive Order 13636

#ccubedvp

WHAT IS THE CRITICAL INFRASTRUCTURE CYBER COMMUNITY?

Directives in Executive Order 13636:

- Community of interest around managing cyber risk

- Builds on years of our experience partnering with industry
  - Previous industry collaborations: risk assessments for IT, Emergency Services, National Public Safety Broadband Network, and many others

- Place for industry, State and local governments, and many other organizations to identify cyber risk management needs and solutions

Transform Increased Interest → Increased Action

#ccubedvp

PROGRAM ACCOMPLISHMENTS

120K+
website visits

310
industry briefings

17 webinars reaching
2,500+
people

600
attendees at 4 regional workshop

#ccubedvp

CENTRAL WEBSITE FOR RESOURCES

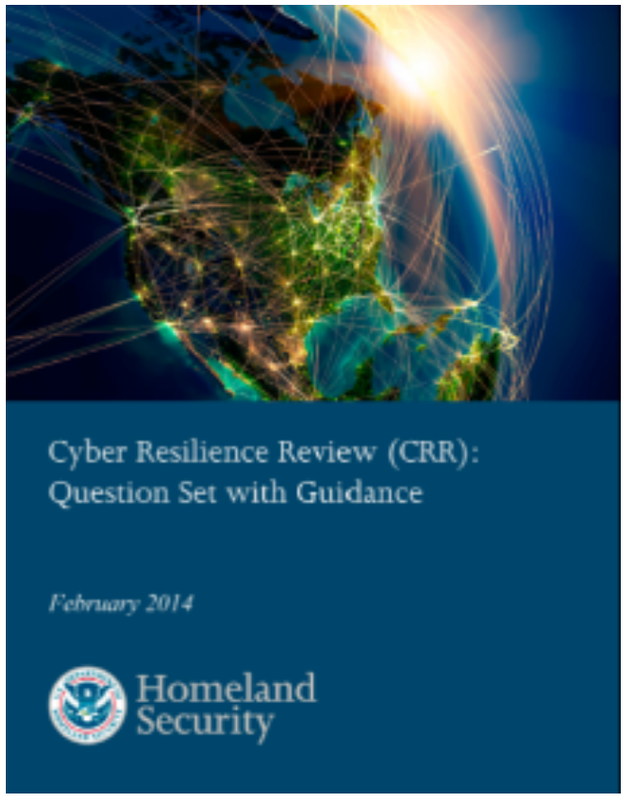
- Over 40 resources currently featured, including the Cyber Resilience Review (CRR)
- Resources are organized by Framework Function
- Pages are organized by stakeholder group:
  - Academia
  - Business
  - Federal
  - State, Local, Tribal, and Territorial (SLTT) government
  - Small and Midsize Business (SMB)

#ccubedvp

PROGRAM RESOURCES

Cyber Resilience Review (CRR)

- A no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices.



Cyber Security Advisors (CSAs)

- Regionally located DHS personnel who direct coordination, outreach, and regional support to protect cyber components of critical infrastructure and State, local, territorial, and tribal (SLTT) governments.

PROGRAM RESOURCES, contd.

Cyber Information Sharing and Collaboration Program (CISCP)

- Leverages government and industry subject matter expertise to collaboratively respond to cybersecurity incidents for unclassified information

Enhanced Cybersecurity Services (ECS) program

- Supports sensitive and classified information sharing to improve the protection of critical infrastructure systems from unauthorized access, exploitation, or data exfiltration

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

- Incident response services to critical infrastructure asset owners that are experiencing impacts from cyber attacks.
- Services include:
  - Analyzing digital media and malware
  - Identifying source of an incident,
  - Analyzing the extent of the compromise
  - Developing strategies for recovery and improving defenses.

2016 GOALS

1. Harmonizing Cybersecurity Risk Management Strategies

2. Building Relationships among Cybersecurity Stakeholders

3. Creating a National Cybersecurity Culture

#ccubedvp

GET INVOLVED

- Check out the website: www.us-cert.gov/ccubedvp
- Sign up for the monthly bulletin *(located at bottom of website)*
- Spread the word in your networks
- Share with us a NIST Framework success story or a valuable resource
- RSVP to our May 5 webinar and to our June 1 Regional Workshop in Indianapolis at CCubedVP@hq.dhs.gov

www.US-CERT.gov/CCubedVP

#ccubedvp

WELCOME TO THE
COMMUNITY.

#ccubedvp

dhs.gov/ccubedvp