Critical Infrastructure Protection Disaster Response Resources

The Critical Infrastructure Protection branch is the agency lead for the Healthcare and Public Health Sector. Key activities within the branch include infrastructure risk analysis and prioritization, cybersecurity initiative coordination for HHS, emergency operation liaison with private sector partners during emergencies, and sector lead for developing, evaluating, and implementing protection measures related to critical infrastructure all hazards threating government and private sector partners.

The Critical Infrastructure Protection branch can provide SME support for partners needing advice or guidance on best practices for physical and cyber critical infrastructure protection.

Requests for SME support should be sent through REC to cip@hhs.gov.

The Critical Infrastructure Protection (CIP) team has a wide network of public and private sector partners representing all aspects of healthcare and public health critical infrastructure protection with expertise in cybersecurity, physical security, workforce protection, supply chain management, and other related areas. During steady-state or disaster operations, CIP can tap into its private sector partners in the following healthcare and public health sub-sectors:

Health IT and Medical Technology
Pharmaceuticals, laboratories, and blood
Medical materials
Health Plans and Payers
Direct Health Care
Mass Fatality Management

Opportunity for two-way sharing of information with national-level private sector partners

Requests to share information or request information from our partnership network should be communicated through the REC to cip@hhs.gov.

The Critical Infrastructure Protection (CIP) team has a wide network of public and private sector partners representing all aspects of healthcare and public health critical infrastructure protection with expertise in cybersecurity, physical security, workforce protection, supply chain management, and other related areas. During steady-state or disaster operations, CIP can tap into its private sector partners in the following healthcare and public health sub-sectors:

Health IT and Medical Technology
Pharmaceuticals, laboratories, and blood
Medical materials
Health Plans and Payers
Direct Health Care
Mass Fatality Management

Connection to all 16 sectors of the national critical infrastructure community, to assist with infrastructure interdependency issues (power, water, communications, etc.)

Requests to share information or request information from other sectors should be communicated through the REC to cip@hhs.gov.
HHS' Critical Infrastructure Protection program is part of the National Infrastructure Protection Program, facilitated by DHS. This connects HHS with 15 other sectors of infrastructure, including:

Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems

Provide threat information to public health departments with classified communications abilities.

CIP manages the State Health Official Clearance Program by which State Health Officials may be nominated for clearances and, in turn, nominate two other individuals from their state. After being approved to review classified materials, the state participants will be invited to annual healthcare and public health classified briefings and may be able to purchase telecommunications equipment that would let them share classified information over the phone. For more information, please contact cip@hhs.gov.

Connection to steady-state and incident information on the Homeland Security Information Network (HSIN)

The Homeland Security Information Network for the Healthcare and Public Health community (HSIN-HPH) is the nation's primary web portal for public / private collaboration to protect its critical infrastructure and resources. It is the primary means by which the Departments of Homeland Security (DHS) and Health and Human Services (HHS) share sensitive but unclassified (SBU) information with their trusted partners. Through HSIN-HPH, users have access to:

Timely, relevant and actionable information about threats, vulnerabilities, security, policy, cybersecurity, and incident response and recovery activities affecting the HPH community
Alerts and notifications of credible threats
Best practices for protection and preparedness measures for HPH stakeholders

Critical Infrastructure Protection (CIP) preparedness and resilience analysis and research products
Communication and collaboration with other subject matter experts

How to Access HSIN-HPH:

To request access to HSIN-HPH, please visit: https://connect.hsin.gov/hph/event/registration.html and complete the online application.

For questions or technical assistance regarding access to HSIN, please contact the HSIN Helpdesk at (866) 430-0162 or send an email to HSIN.helpdesk@dhs.gov.

For questions specifically regarding HSIN-HPH, please contact the HPH Sector Specific Agency at cip@hhs.gov.

Last Updated: June 24, 2015