



United States Department of

Health & Human Services

Office of the Assistant Secretary for Preparedness and Response (ASPR)



Critical Infrastructure Protection for the Healthcare and Public Health Sector

David Morgan and Steve Curren

June 17, 2009

SARMA Conference, Arlington, VA



United States Department of

Health & Human Services

Office of the Assistant Secretary for Preparedness and Response (ASPR)



Presentation Outline/Objectives

- Brief description of critical infrastructure protection (CIP)
- Overview of national strategy and organizational structures for CIP
- Unique challenges in applying CIP to the Healthcare and Public Health Sector
- Risk assessment for Healthcare and Public Health Sector
- Action agenda for risk mitigation



Critical Infrastructure Definitions

- Critical Infrastructure Protection (CIP) - *the strategies, policies, and preparedness needed to protect, prevent, and when necessary, respond to attacks on these sectors' critical infrastructure and key resources.*
- Critical Infrastructure (CI) and Key Resources (KR) – *the assets, systems, networks, and functions, whether physical or organizational, whose destruction or incapacity would have a **debilitating** impact on the Nation's security, the public's health and safety, and/or economic vitality.” These resources are “publicly or privately controlled resources essential to the minimal operations of the economy and government.”*
- Resiliency - *the ability of an asset, system, network, function, to maintain its capabilities and functioning during and in the aftermath of an All-Hazards incident.*



Plans to Meet the Sector Goals

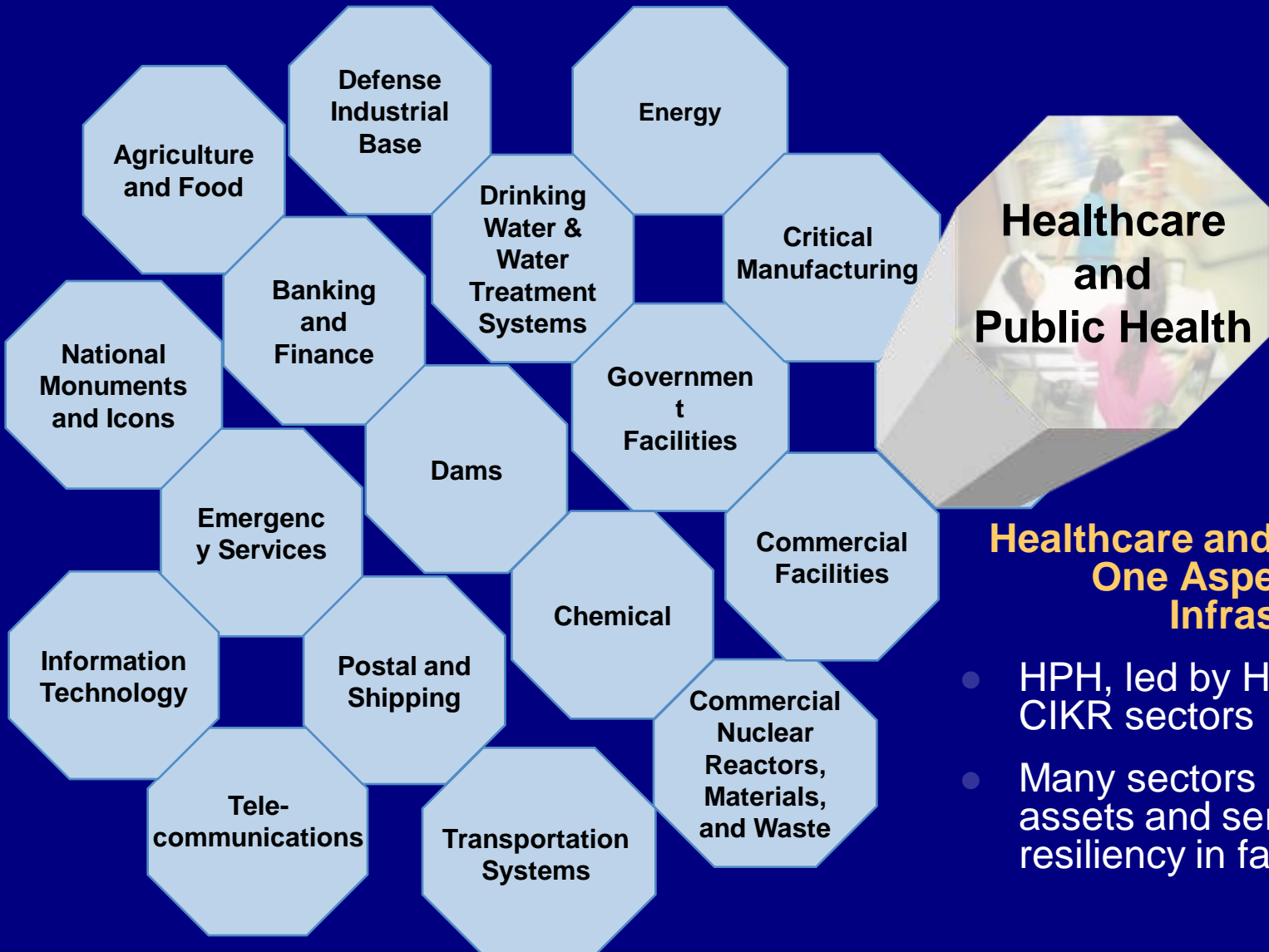
Homeland Security Presidential Directive 7 (HSPD-7)

National Infrastructure Protection Plan
Partnering to enhance protection and resiliency
2009

Homeland Security

Public Health & Healthcare
Critical Infrastructure and Key Resources
Sector-Specific Plan as input to the
National Infrastructure Protection Plan
May 2007

Homeland Security Department of Health and Human Services



Healthcare and Public Health: One Aspect of Critical Infrastructure

- HPH, led by HHS, one of 18 CIKR sectors
- Many sectors rely on HPH assets and services to ensure resiliency in face of threats



HPH Sector Structure

Sector Specific Agency (HHS)

Healthcare Sector Coordinating Council (HSCC)

The HSCC is comprised of representatives and alternates from each sub-council. Issues will be identified by Subcouncils. Coordination across Subcouncils and with the HPHGCC will be organized through the HSCC.

Government Coordinating Council

Cross-cutting Work Groups will be established to address priority issues that cut across sub-councils

Direct Health Care

Health Plans and Payers

Pharmaceuticals, Laboratories, and Blood

Medical Materials

Mass Fatality Management

Health Information and Medical Technology

Each sub-council is responsible for organizing itself

Sample Priority Issues for Sub-Councils: Emergency Preparedness, Emergency Response; Vulnerability Assessment / Prioritization; Communication & Information Sharing among members, with HHS and DHS, and with other sectors



Unique Tools

- Critical Infrastructure Protection Advisory Council (CIPAC)
 - Allows flexibility for industry/industry and industry/government coordination for infrastructure protection
 - Requires adherence to CIPAC policies and procedures
- Protected Critical Infrastructure Information (PCII)
 - Allows for sharing of information between the private sector and federal government
 - Restricts sharing of information to homeland security purposes
 - Provides legal protections from public disclosure
 - ❖ Freedom of Information Act (FOIA)
 - ❖ Civil Litigation



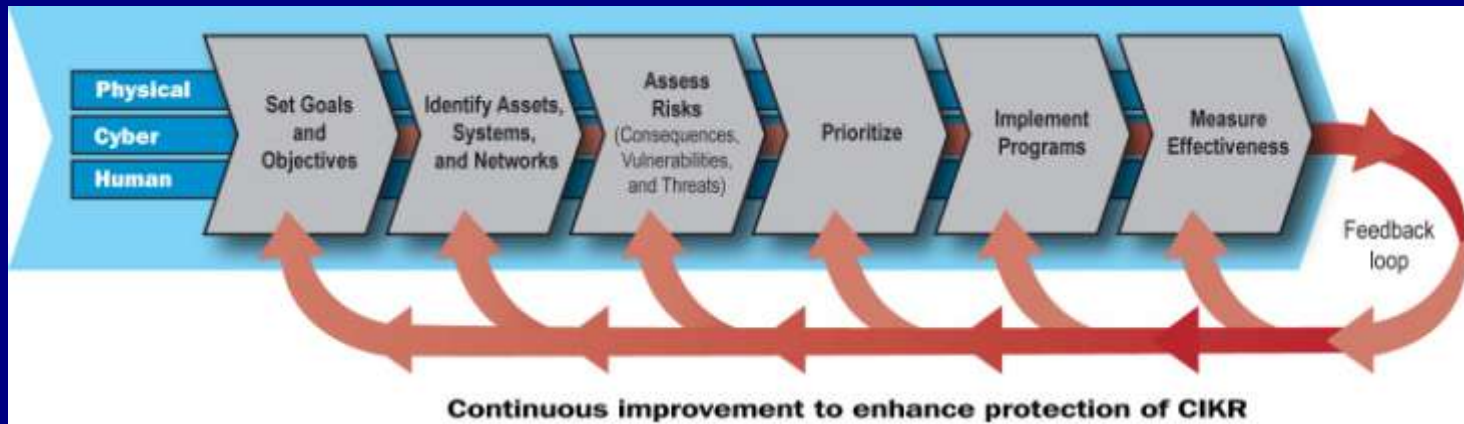
Planning Documents

- National Infrastructure Protection Plan
 - Established by Homeland Security Presidential Directive 7
 - Latest version released early 2009
- Sector Specific Plan (SSP) – CUI and UNCLAS
 - Re-written tri-annually
 - Due for completion in December 2009
 - Updated/revised as necessary
 - Requires approved from the Secretary of HHS, DHS, and WH HSC
 - Submitted to POTUS
 - Both CUI and UNCLAS versions developed
- Sector Annual Report (SAR) – CUI and UNCLAS
 - Completed annually
 - Becomes an appendix to the National Annual Report (NAR)
 - Both CUI and UNCLAS versions developed
- National Annual Report (NAR) – Classified
 - Includes all 18 SARs in addition to consolidated assessments of the individual reports
 - Includes the National Terrorism Risk Profile
 - Submitted to WH HSC and POTUS



Risk Management Framework

- The NIPP describes processes to:
 - Set Goals and Objectives
 - Identify Assets, Systems, and Networks
 - Assess Risk (Consequences, Vulnerabilities, and Threats)
 - Prioritize
 - Implement Protective Programs & Resiliency Strategies
 - Measure Effectiveness
- IP develops methodologies with and for its partners for risk assessment, risk prioritization, and performance measurement
- The Sector-Specific Plans tailor these processes for each sector and describe sector-specific approaches and methodologies





United States Department of

Health & Human Services

Office of the Assistant Secretary for Preparedness and Response (ASPR)



HPH Sector Goals

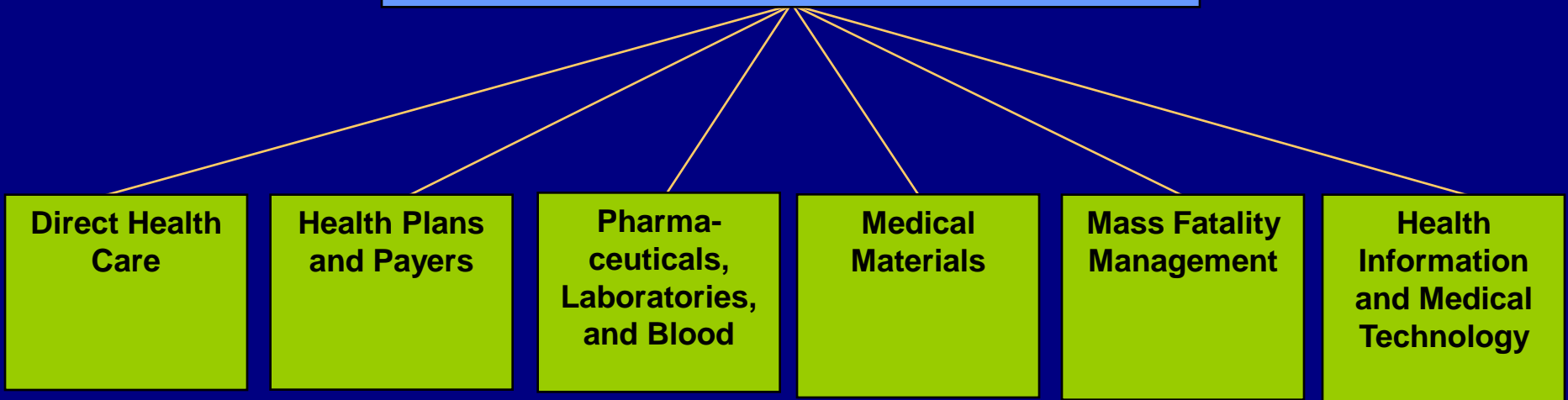
- Continuity of Services
- Workforce Protection
- Physical Security
- Cyber Security



HPH Sector Assets, Networks, and Systems

Healthcare Sector Coordinating Council (HSCC)

The HSCC is comprised of representatives and alternates from each sub-council. Issues will be identified by Subcouncils. Coordination across Subcouncils and with the HPHGCC will be organized through the HSCC.





Sector Risk Assessment Process

- Strategic Homeland Infrastructure Risk Assessment (SHIRA)
 - National Terrorism Risk Profile
 - Sector Terrorism Risk Profile
 - State Terrorism Risk Profile
 - Cybersecurity
- Protected Critical Infrastructure Information (PCII)
 - Identification of vulnerabilities without disclosing them
 - Protection of sensitive industry information
 - Collection of data on important infrastructure issues
 - ❖ Supply chain
 - ❖ Healthcare facility capacity/status
 - ❖ Mitigation activities
 - ❖ Response and recovery plans



HPH Sector Risks

- Continuity of Services
 - Supply chain interruptions
 - Surge demands
 - Example: 2004-2005 influenza vaccine shortage
- Workforce
 - Indirect exposures
 - Example: Pandemic threat to healthcare personnel
- Physical Assets
 - Direct attacks
 - Theft of biological select agents and toxins (BSAT)
 - Example: Attack on Cama Hospital, Mumbai
- Cyber Systems
 - Service interruption
 - Data theft and fraud
 - Example: Conficker worm



Setting Priorities:

HPH Sector Joint Advisory Working Groups

- Risk Assessment (New for 2009)
 - Tier 1 / Tier 2 data call
 - CFDI data call
 - Asset prioritization
- Research and Development
 - Capability gaps
 - Research priorities
- Information Sharing (New for 2009)
 - Information sharing needs and priorities
- Workgroup Structure
 - New members always welcome
 - Some working groups require a security clearance
 - HHS can obtain clearances for individuals who are interested in participating



HPH Sector Mitigation Programs

- Continuity of Services
 - HHS Hospital Preparedness Program
 - CDC Public Health Emergency Preparedness Program
 - FDA Drug, Biologic, and Medical Device Shortage Program
 - Private sector programs (e.g., RxResponse)
- Workforce Protection
 - Disease detection and investigation
 - SNS and Cities Readiness Initiative
- Physical Security
 - CDC Select Agent Program
 - Hospital protection standards (e.g., Joint Commission)
- Cyber Security
 - Sector information sharing



Federal CIP Initiatives

- Enhanced Critical Infrastructure Protection (ECIP) Site Visits
 - Includes SLTT partners, HHS Regional Emergency Coordinators, and DHS Protective Security Advisors
 - Conducted on all Tier 1 assets annually
 - Conducted on Tier 2 assets as time permits and need is established
- Site Assistance Visit
 - Vulnerability assessment and identification tool
 - Includes completion of a self-assessment
- Information Sharing



Measuring Effectiveness of HPH Sector Mitigation Programs

- HPH Sector Annual Report
- Programmatic Metrics
- ECIP/SAV Reports
- NO NEW METRICS!
- Examples:
 - Increased participation in RxResponse from 3 to 21 states
 - Increased number of metropolitan statistical areas meeting Cities Readiness Initiative criteria by 30%
 - Doubled the number of security site audits at medical countermeasure facilities



HPH Sector Priorities

- Information Sharing
 - Homeland Security Information Network (HSIN)
 - Threat briefings
 - Protected Critical Infrastructure Information (PCII)
- Response Coordination
 - Private Sector Liaison Officer (LNO)
 - Sector conference calls
 - HSIN incident pages
- Awareness and Expansion
 - SCC outreach
 - HSIN roll-out
 - Technical assistance for state/local CIP programs



Next Steps

- Beginning annual production cycle for all sector-based initiatives
 - New members always welcome
- Expand private sector engagement into Federal initiatives (National Biosurveillance Strategy, NBSB, and research projects)
- Continue HSIN enrollment for sector partners
 - Promulgation of enrollment process into the states
- Continue obtaining clearances for sector partners involved in select CIP activities
- Schedule open and secure briefings at key HPH sector partner meetings (DHP meetings, annual preparedness conference, etc)
- Obtain SLTT input on customized intelligence products for the sector



Questions



David Morgan

HPH SCC Co-Chair

Owner, Brooklawn Memorial Park

Portland, ME

david@brooklawnmp.com

Steve Curren

Deputy Program Manager, CIP

US Dept of Health & Human Services

Washington, DC

Stephen.Curren@hhs.gov