

Critical Infrastructure Protection for the Healthcare and Public Health Sector

Nitin Natarajan
Program Manager, CIP
Office of Preparedness and Emergency Operations
February 20, 2009

ASTHO/NACCHO Preparedness Summit

United States Department of Health & Human Services
Office of the Assistant Secretary for Preparedness and Response (ASPPR)

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

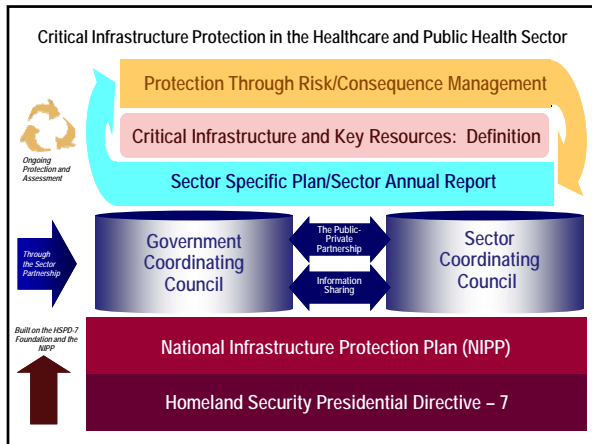
1

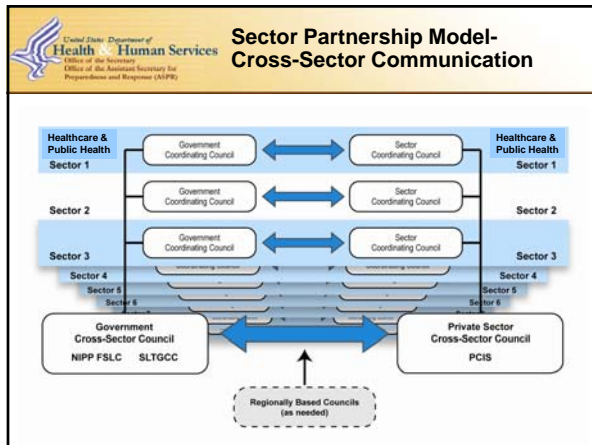
United States Department of Health & Human Services
Office of the Assistant Secretary for Preparedness and Response (ASPPR)

HPH 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.*

2





United States Department of Health & Human Services
Office of the Assistant Secretary for Preparedness and Response (ASPPR)

Plans to Meet the Sector Goals

National Infrastructure Protection Plan
2006
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

Emergency Operations

- HHS CIP serves as sector liaison to the National Infrastructure Coordination Center (NICC)
- HHS CIP is a member of the HHS Emergency Management Group (EMG) and HHS Emergency Response Group (ERG) (COOP)
- Three avenues for private sector partners to share information or submit event or disaster related RFI's into the IP system
 - Through the NICC
 - Through the Sector Specific Agency (SSA) – HHS
 - Through local/state channels (HIGHLY ENCOURAGED)
- Opportunity for local SCC members to serve as liaisons in the HHS Secretary's Operations Center (SOC) and the DHS National Infrastructure Coordination Center (NICC)
- Participate on all key HHS, DHS, and FEMA incident related conference calls

Cybersecurity

- Component of tripartite HHS group to address Healthcare and Public Health cybersecurity issues both internal and external to HHS
- Works closely with DHS on the components of the President's Cybersecurity Initiative as required by HSPD-23
 - Twelve identified "initiatives"
 - Initiatives 11/12 pertain to the private sector/SLTT integration
 - Initiative 12 is nearing completion with products to be released shortly
- Seeking additional SLTT SME's to assist in this initiative

HPH Sector Joint Advisory Working Groups

- Include private/public sector (SLTT) partners and academia
- Two existing working groups
 - Research and Development Working Group
 - Sector Specific Metrics Working Group
- Two new working groups being formed in FY2009
 - Information Sharing Working Group
 - Risk Assessment Working Group
- New members always welcome
- Some working groups require a security clearance
 - HHS can obtain clearances for individuals who are interested in participating

Research and Development

- Utilizes the Joint Advisory Working Group for Research and Development (JAWG R&D)
 - Co-chaired by the private sector and academia
 - Meets regularly throughout the year
 - Includes members of the government, private sector, and academia
 - State/local membership desired
- Identification of key preparedness, response, and recovery capability gaps throughout the sector
- Gaps utilized as prioritized project list for various sources including HHS, DHS, and academia
 - In FY2008 five gaps funded by DHS and one funded by HHS

12

Metrics

- Measure Progress of Protective Efforts within the Sector
- NO NEW METRICS!
- Programmatic Metrics
 - Defined by DHS & SSA - based on SSP and SAR goals & objectives
 - Submitted semi-annually
- Sector-specific Metrics
 - Under development - will be based upon existing metrics & data
 - Metric definitions due to DHS in Spring, 2009
 - First data reporting due to DHS in Spring, 2010

13

Information Sharing

- Sharing of unclassified and classified preparedness, response and recovery information with our private sector partners and state/local government
 - Distribution of reports via electronic or physical means as available
 - Working with DHS to develop a "Reading Room" in the NCR
 - Will be delivering open source and secure briefings for state/local partners
- Identification of key private sector/SLTT reports which are voluntarily shared with the federal government (i.e. – situation reports/executive summaries) for dissemination among the HPH community
- Work with the IC for the development of UNCLAS, CUI, and classified HPH sector specific intelligence products
 - SLTT input desired to ensure that the products are helpful

14

United States Department of Health & Human Services
Office of the Assistant Secretary for Preparedness and Response (ASPPR)

Information Sharing

•HSDN Access available at most HSA offices
•Working with DHS for alternatives (USSS/other federal agencies)

•HSIN Access readily available
•CUI E-mail includes use of CUI Rules, PKI, etc

UNCLAS

CUI

SECRET

Delivery Notice ONLY

HSDN SIPRNET

HSIN CUI E-mail

UNCLAS E-mail

15

United States Department of Health & Human Services
Office of the Assistant Secretary for Preparedness and Response (ASPPR)

“Core” Information Sharing Capabilities – Platform Determination

RC&C

A&N

SAR

DM

IC&C

Core CIS Capabilities

- **Governance and Membership Foundation:**
 - Sector and SCC/GCC Charters and organizational policies identify the Sector’s membership and operating policies.
- **Core Information Sharing Capabilities:**
 - **Alerts, Warnings & Notifications (AWN):** Details how the sector will receive and distribute notices provided by the government and industry analysts to the sector.
 - **Suspicious Activity Reporting (SAR):** Details how the sector will receive and distribute reports of suspicious activity affecting critical infrastructure.
 - **Data Management (DM):** Details how the sector will develop, post, distribute and maintain documents and other forms of data.
 - **Incident Collaboration & Communication (IC&C):** Details how the sector will communicate during an emergency or incident.
 - **Routine Collaboration & Communication (RC&C):** Details how the sector will communicate during non-emergency situations.

Developing and documenting governance and core information sharing capabilities allows CIKR Sectors and their partners to achieve robust information sharing for critical infrastructure protection.

15

United States Department of Health & Human Services
Office of the Assistant Secretary for Preparedness and Response (ASPPR)

HSIN “Next Generation”

- Current *User Interface* is virtually unchanged for users, providing a seamless integration and transition.
- *Security Infrastructure* is deployed in front of the legacy MS SharePoint application. The legacy HSIN CS login remains but can be supplemented with a new, two-factor authentication login.
- *New User Functionality* is delivered via Adobe Acrobat Connect - a robust collaborative environment with real-time online presentation capability, file sharing, chat and user presence awareness.
- *Alerts and Notifications* are managed via L-Soft List Serv to allow management of announcement lists, delivery of messages, users to automatically subscribe / unsubscribe, and maintain their subscription settings through a web interface.
- *Bulk upload* capability enables incorporation of groups of members into Sector or Sector Council portal environment.

17



Risk Assessment

- Strategic Homeland Infrastructure Risk Assessment (SHIRA)
 - National Terrorism Risk Profile
 - Sector Terrorism Risk Profile
 - State Terrorism Risk Profile
 - Cybersecurity
- Tier 1/2 asset criteria development/identification
- Critical Foreign Dependencies Initiative (CFDI)
 - Identifies key foreign interdependencies as it related to the HPH sector
 - Primarily in the production and manufacturing arena
- FBI Critical National Assets (CNA) Program
 - National Counterintelligence Working Group



ECIP/SAV

- Enhanced Critical Infrastructure Protection Visit
 - 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
- Data is being standardized
- Custom sector specific reporting in FY2009
- Comparisons between sectors available in FY2009



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 (DPPH meetings, annual preparedness conference, etc)
- Obtain SLTT input on customized intelligence products for the sector

Questions



Nitin Natarajan
Program Manager, CIP
Dept of Health and Human Services
202-260-2002 Office
703-200-6728 Cellular
Nitin.Natarajan@hhs.gov E-mail

Steve Curren
Deputy Program Manager, CIP
202-260-1241 Office
202-281-8039 Cellular
Stephen.Curren@hhs.gov E-mail
