National Health Critical Infrastructure Resilience

The National Health ISAC
Presidential Directive (HSPD-7)

Identify, Prioritize, Protect

National Critical Infrastructures

National Infrastructure Protection Plan (NIPP)

Protection Efforts and Resiliency

Sector-Specific Agencies (SSAs) + Plans

Information Sharing & Analysis Centers (ISACs)
Relies on a Sector Partnership Model

- National-Level Organizational Structure
- Public/Private Policy and Planning Coordination *Within* and *Across* All Sectors
- Coordinating Councils -
  - Government Coordinating Council (GCC)
  - “Private” Sector Coordinating Council (SCC)
- Information Sharing & Analysis Centers (ISACs)
EMERGENCY SUPPORT FUNCTIONS / COORDINATORS

ESF #1 - Transportation (Dept. of Transportation)

ESF #2 - Communications (DHS)

ESF #3 - Public Works and Engineering (DoD)

ESF #4 - Firefighting (Dept. of Agriculture - US Forest Service)

ESF #5 - Emergency Management (DHS - FEMA)

ESF #6 - Mass Care, Emergency Assistance, Housing/Human Services (DHS - FEMA)

ESF #7 - Logistics Management and Resource Support - (GSA and DHS (FEMA)

ESF #8 - Public Health and Medical Services - (Dept. Health and Human Services)

ESF #9 - Search and Rescue (DHS - FEMA)

ESF #10 - Oil and Hazardous Materials Response - EPA

ESF #11 - Agriculture and Natural Resources - Dept. of Agriculture

ESF #12 - Energy - Dept. of Energy

ESF #13 - Public Safety and Security - Dept. of Justice

ESF #14 - Long-Term Community Recovery (DHS - FEMA)

ESF #15 - External Affairs (DHS)
Formed in Response to a Presidential Directive

Private-Sector Led

Nationally Recognized

Federal Sector-Specific agency (SSA)

Sector’s Coordinating Council (SCC)

Intelligence Agencies | Law Enforcement

National Council of ISACs

Critical Infrastructure Owners and Operators.

Communications ISAC (NCC), Electric Sector ISAC (ES-ISAC), Emergency Management & Response ISAC (EMR-ISAC), Financial Services ISAC, Health ISAC (NH-ISAC), Highway ISAC (First Observer), IT ISAC

Maritime Security Council ISAC, Multi-State ISAC, Nuclear ISAC (NEI), Public Transportation ISAC (APTA), Real Estate ISAC, Research & Education Networking ISAC (REN-ISAC), Supply Chain ISAC (SC-ISAC)

Surface Transportation ISAC (ST-ISAC), Water ISAC, Chemical Sector Coordinating Council, Defense Security Information Exchange, Oil and Natural Gas Coordinating Council, Partnership for Critical Infrastructure Security, Regional Consortium Coordinating Council
National Information Sharing & Analysis Centers (ISACs)

As defined by the National Infrastructure Protection Plan (NIPP)

“ISACs are privately-led sector-specific organizations advancing physical and cyber security critical infrastructure and key resources (CI/KR) protection by establishing and maintaining collaborative frameworks for operational interaction between and among members and external partners.”

ISACs - Cybersecurity Tactical + Operational Arm - Nationally Recognized

Sector-Specific Federal Agency (SSA), Sector-Coordinating Council (SCC), Intelligence Agencies (DHS, FBI), The National Council of ISACs and critical infrastructure owners/operators.

Security Intelligence - Sector-and Cross-Sector Situational Awareness Information Sharing Threats and Vulnerabilities, Incident Response, Leading Practice and Education 

Establishing Operational-Level Dialogue with Appropriate Government Agencies
NH-ISAC MISSION

To enable, ensure and preserve the public trust, advancing resilience of the Nation’s Healthcare and Public Health Critical Infrastructure

• Trusted Cybersecurity and All Hazards Security Intelligence
• Sector-Specific and Cross-Sector Analysis
• Early Warnings, Notifications
• Countermeasure Solutions / Incident Response
• Fostering the Availability of Proven Security Governance, Awareness and Education

NH-ISAC – Nationally Recognized
National Council of ISACs

National Sector Coordinating Council (SCC), Chair, Healthcare Cyber Legislation Committee

DHS Cyber Unified Coordination Group (UCG) - Appointed by US HHS
DHS National Critical Infrastructure Protection Advisory Council (CIPAC)
National Cyber Security Council - Board Appointment

NH-ISAC MISSION
The White House
Office of the Press Secretary

For Immediate Release

February 12, 2013

Presidential Policy Directive -- Critical Infrastructure Security and Resilience

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.
Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY
• Adequately Define Outcomes to Strengthen Cybersecurity and Support Business Objectives

• Enable Cost-Effective Implementation

• Integrate Cybersecurity Risk into Business Risk

• Provide Tools for Sr. Executives and Boards of Directors to Understand Risks & Mitigations

• Provide Sufficient Guidance and Resources While Maintaining Flexibility

• Provide Specific Focus and Guidance for Mitigating Impact of Cybersecurity Measures on Privacy and Civil Liberties

• Express Existing Practices To Allow for Effective Use
April 2013 – US Dept. of Commerce, DC

May 2013 - Carnegie Mellon University, Pittsburgh, PA

July 2013 – National Health ISAC + UC San Diego

Sept. 2013 – University of Texas, Dallas

November 14-15 – University of NC, Raleigh
Improving Critical Infrastructure Cybersecurity
Executive Order 13636

Preliminary Cybersecurity Framework

http://www.nist.gov/itl/cyberframework.cfm
FRAMEWORK CORE

Cybersecurity Activities | References – Common Across Critical Infrastructures

Cybersecurity Risk From Board Level to Operational Level

5 Functions: Identify | Protect | Detect | Respond | Recover

Function Categories + Subcategories – Standards/Leading Practice

Privacy & Civil Liberties Methodology

FRAMEWORK PROFILE

Outcomes Achieved or to be Achieved - Alignment of Best Practice.

FRAMEWORK IMPLEMENTATION TIERS –


(NH-ISAC) National Health Cybersecurity Resilience
<table>
<thead>
<tr>
<th>FRAMEWORK CORE</th>
<th>FUNCTIONS</th>
<th>CATEGORIES</th>
<th>SUBCATEGORIES</th>
<th>INFORMATIVE REFERENCES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IDENTIFY

Develop Understanding to Manage Cyber Risk for Systems, Assets, Data, Capabilities.

Outcome Categories –

Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy

PROTECT

Develop, Implement and Prioritize Appropriate Safeguards (Risk Management)

Outcome Categories –

Access Control, Awareness & Training, Data Security, Information Protective Processes/Procedures, Protective Technology
DETECT

Develop and Implement the Appropriate Activities to Identify Cyber Event.

Outcome Categories – Anomalies, Events, Security Monitoring, Detection Processes

RESPOND

Develop, Implement and Prioritize Appropriate Activities (Risk Management) to Take Action Regarding Cyber Event

Outcome Categories – Response Planning, Analysis, Mitigation, Improvements

RECOVER

Develop, Implement and Prioritize Appropriate Activities (Risk Management) to Restore Capabilities or Service Impacted

Outcome Categories – Recovery Planning, Improvements, Communications
National Health Cybersecurity Resilience Partnership (NH-CRP)

NATIONAL HEALTH CYBERSECURITY RESILIENCE FRAMEWORK (NH-CRF)

DEFINED BY THE HEALTH SECTOR

NATIONAL HEALTH CYBERSECURITY COMMUNICATIONS AND CONTROL (NC-NCC)

NATIONAL HEALTH CYBERSECURITY FIRST RESPONDERS (NH-CFR)

NATIONAL HEALTH CYBERSECURITY EDUCATION (NH-CFE)
STATE-SPECIFIC COUNCILS

PUBLIC/PRIVATE

HEALTH + EMERGENCY RESPONSE STAKEHOLDERS

INITIAL WEBINAR / STATE-WIDE WORKSHOP
• Trusted Entity – Established By and Sustained by the Health Sector

• Policy – Helping Government Understand HPH Sector Impacts

• Secure Operations – 24/7 Cyber and All-Hazards Security Intelligence

• Cross-Sector Analysis / Information Response

• National Health Cybersecurity Resilience Exercises

• Security Risk Management / Leading Practice

• Awareness / Workforce Education
8 CORE CONSTRUCTS

- Cyber Observable – IP Address, Registry Key Value, File Deletion, etc.
- Indicator – Set of related system and network activity
- Incidents – Instances of specific adversary actions
- TTP – Tactics, Techniques and Procedures
- Exploit Target – Something about a potential victim (weakness, vulnerability)
- Courses of Action – Prevent, Mitigation, Remediate
- Cyber Attack Campaigns – Sets of incidents or TTP with a shared intent
- Cyber Threat Actors – Adversary Identification and/or characterization
NATIONAL HEALTH CYBERSECURITY INTELLIGENCE

Private Sector Information Sharing

Intelligence Feeds
Internet/Media

NH-ISAC Members
Health Sector
Cross-Sector CIKR
Nat’l Council of ISACs
Security Intelligence + Technology Vendors

Government Information Sharing
Fed/State/Local
US HHS
US DHS, US-CERT, FBI

NH-ISAC Analyst
US DHS – NCCIC

Automated Cybersecurity Intelligence Information Sharing

NH-ISAC
STIX Compliant
Security Intelligence Repository
Threat + Vulnerability Analysis, Export/Import Management

Members’ Trusted Threat Information Sharing Portal

© 2013 by NH-IAC, All Rights Reserved. Confidential.
Public / Private Partnership

Planning

Awareness - Interdependencies (Enterprise, Sector and Cross-Sector)

Public/Private Proactive Response | Critical Functions

Resiliency

Delivering Protection, Prevention, Mitigation, Response & Recovery

Mutual Aid Agreements - Eliminating Barriers

Sharing Information

Cyber Threat Two-Way Information Sharing

Security Intelligence - Technical Expertise - R&D

Managing Risk

Sector-Specific Risk Landscapes - Enterprise - Sector - Cross-Sector

Threat and Vulnerability Risk Reduction | Leading Practice

Education (Awareness / Workforce Education)
YOUR OPPORTUNITY TO ENGAGE WITH A DEFINING VOICE IS NOW!

National Health ISAC (NH-ISAC)
Global Situational Awareness Center
NASA Space Life Sciences Laboratory
NASA/ Kennedy Space Center
Deborah Kobza, Executive Director / CEO
d kobza@nhisac.org, 904-476-7858