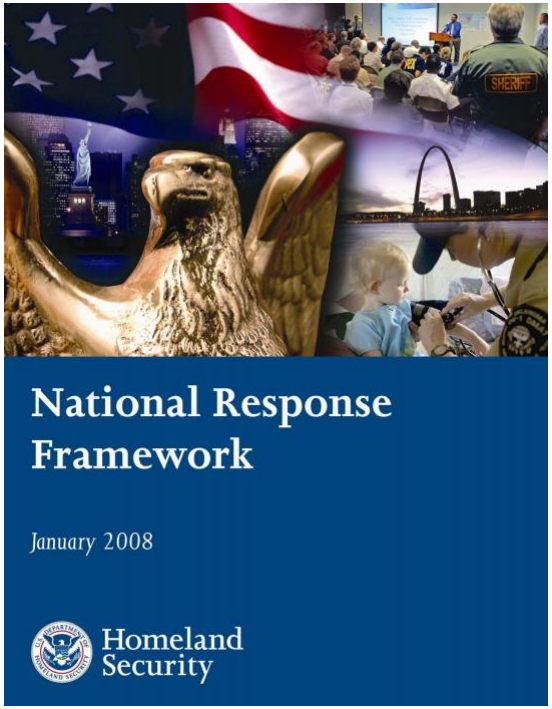
The National Health ISAC (NH-ISAC)

Physical Threats – Cyber Impacts

Physical / Cyber – All Hazards Response



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

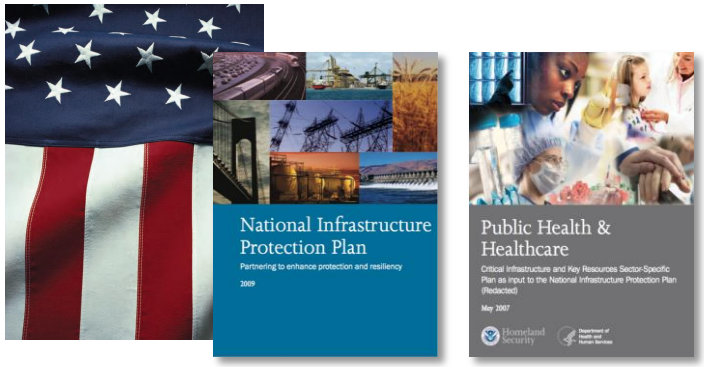
ESF # 12 – Energy – Dept. of Energy

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

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

ESF # 15 – External Affairs (DHS)

National Critical Infrastructures



Presidential Directive (HS

Identify, Prioritize, Protect

National Critical Infrastructures & Key Resources (CI/KR)

National Infrastructure Protection Plan (NIPP)

CI/KR Protection Efforts and Resiliency

Sector-Specific Agencies (SSAs) + Plans

Information Sharing & Analysis Centers (ISACs)

Sector-Specific Agency (SSA)	Critical Infrastructures & Key Resources
Department Of Agriculture Department of Health & Human Services	Agriculture & Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health & Human Services	**Healthcare & Public Health**
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking & Finance
Environmental Protection Agency	Water
Department of Homeland Security (DHS) Office of Infrastructure Protection	Chemical / Commercial Facilities / Dams Critical Manufacturing /Emergency Services Nuclear Reactors, Materials and Waste
DHS Office of Cybersecurity & Communications	Information Technology Communications
DHS Transportation Security Administration	Postal and Shipping
DHS Transportation Security Administration United States Coast Guard	Transportation Systems
DHS Immigration & Customs Enforcement, Federal Protective Service	Government Facilities

National ISAC Infrastructure

Formed in Response to a Presidential Directive

Private-Sector Led

Nationally Recognized

Federal Sector-Specific agency (SSA)

Sector's Coordinating Council (SCC)

Intelligence Agencies

National Council of ISACs

Critical Infrastructure Owners and Operators.

Communications ISAC (NCC), Electric Sector ISAC (IS-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

What is an ISAC

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

Coordinating Councils

Government Coordinating Council (GCC)

- Composition – Federal, State, Local, Tribal, Territorial
- Chair(s) + US DHS Assistant Secretary for Infrastructure Protection or Designee
- Cross-Sector Coordination – Activities, Policy + Communications
- Prepare For, Respond To, Recover From Significant Hazards (Natural and Manmade)

Sector Coordinating Council (SCC)

- Composition – Private Sector CI Owners/Operators/Supporting Organizations
- Chair(s) – Private Sector Elected, Self-Organized, Self-Run, Self-Governed
- Advocate Owners/Operators Interests – Enhance Government Policies, Plans + Actions
- Interaction – Sector-Specific Response Strategies, Policies, Initiatives, Working Groups
- Monthly Conference Call, Semi-Annual In-Person Meetings

Health Sector Coordinating Council (SCC)

Health Sector Coordinating Council (SCC)

Direct Patient Healthcare	Health Information and Medical Technology
Health Plans and Payers	Pharmaceuticals / Laboratories / Blood
Medical Materials	Mass Fatality Management Services

Active Working Groups

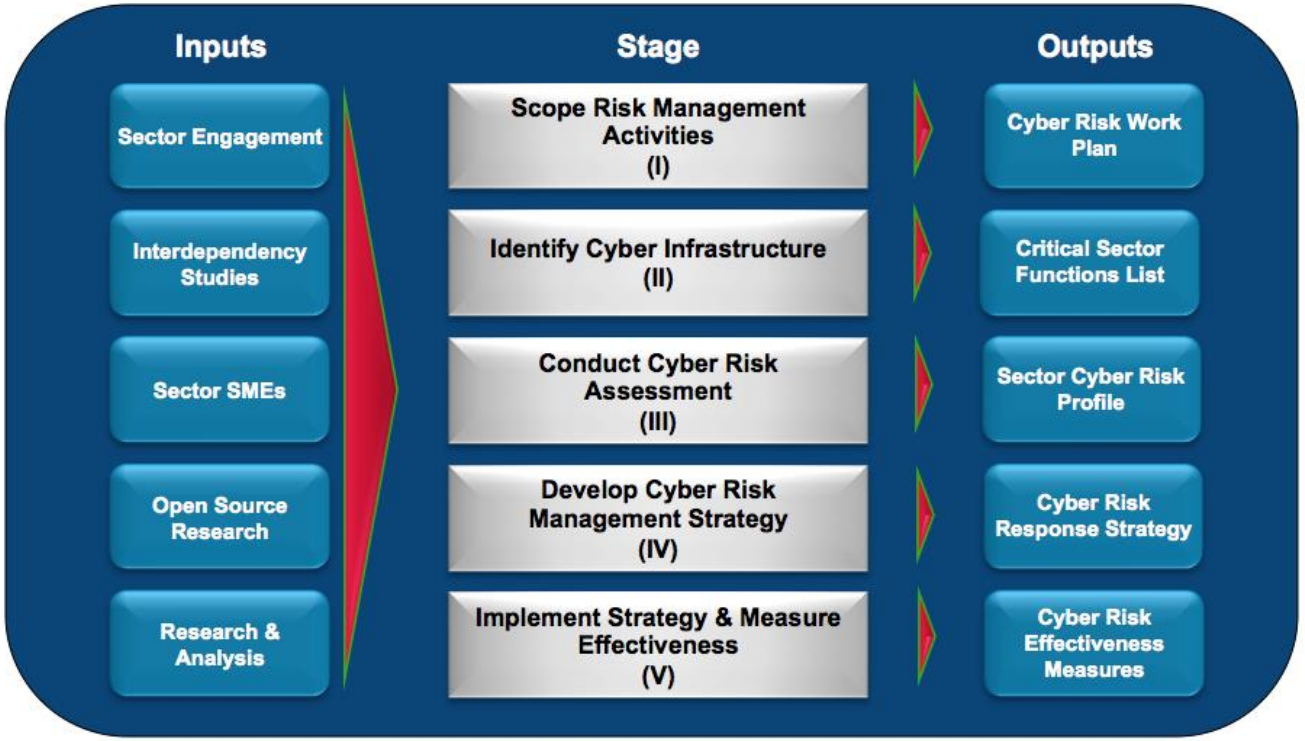
- Information Sharing and R&D Working Group
- Risk and Cybersecurity Working Group

Health Sector Cyber Legislation Committee

- Chair, Deborah Kobza, National Health ISAC

Active Shooter Committee

Cyber Infrastructures



Federal Cybersecurity Policy / Programs

2011 Presidential Policy Directive: PPD-8: National Preparedness

International Strategy for Cybersecurity

National Strategy for Trusted Identities in Cyberspace

National Initiative for Cybersecurity Education

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

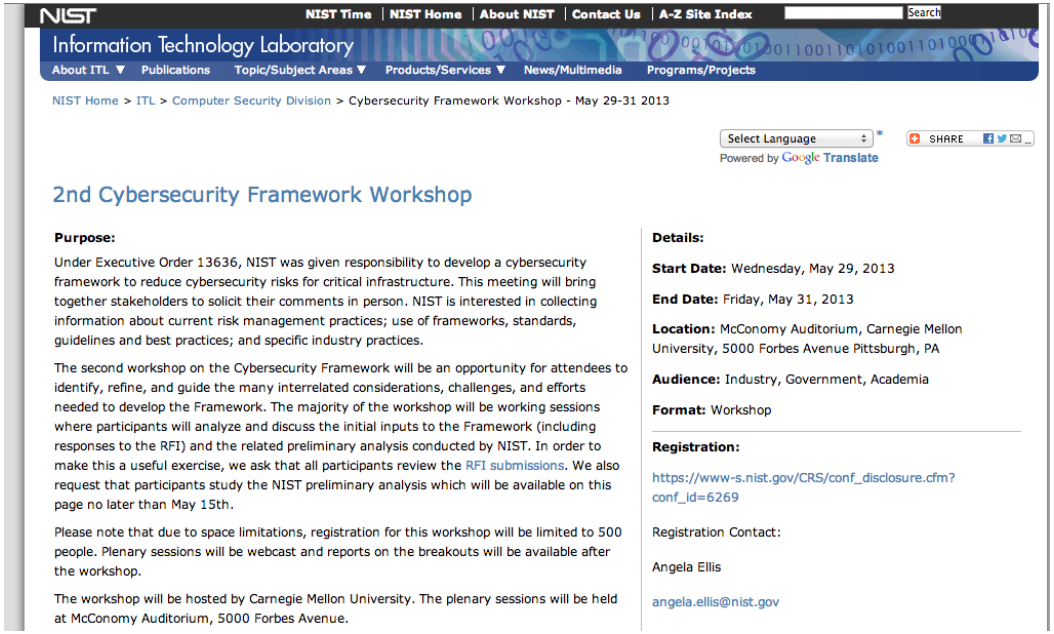
NIST Cybersecurity Framework

Launch Conference

US Department of Commerce

April 2013

500+ Attendees



NIST | NIST Time | NIST Home | About NIST | Contact Us | A-Z Site Index | Search

Information Technology Laboratory

About ITL ▼ | Publications | Topic/Subject Areas ▼ | Products/Services ▼ | News/Multimedia | Programs/Projects

NIST Home > ITL > Computer Security Division > Cybersecurity Framework Workshop - May 29-31 2013

Select Language | SHARE

Powered by Google Translate

2nd Cybersecurity Framework Workshop

Purpose:

Under Executive Order 13636, NIST was given responsibility to develop a cybersecurity framework to reduce cybersecurity risks for critical infrastructure. This meeting will bring together stakeholders to solicit their comments in person. NIST is interested in collecting information about current risk management practices; use of frameworks, standards, guidelines and best practices; and specific industry practices.

The second workshop on the Cybersecurity Framework will be an opportunity for attendees to identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop the Framework. The majority of the workshop will be working sessions where participants will analyze and discuss the initial inputs to the Framework (including responses to the RFI) and the related preliminary analysis conducted by NIST. In order to make this a useful exercise, we ask that all participants review the RFI submissions. We also request that participants study the NIST preliminary analysis which will be available on this page no later than May 15th.

Please note that due to space limitations, registration for this workshop will be limited to 500 people. Plenary sessions will be webcast and reports on the breakouts will be available after the workshop.

The workshop will be hosted by Carnegie Mellon University. The plenary sessions will be held at McConomy Auditorium, 5000 Forbes Avenue.

Details:

Start Date: Wednesday, May 29, 2013

End Date: Friday, May 31, 2013

Location: McConomy Auditorium, Carnegie Mellon University, 5000 Forbes Avenue Pittsburgh, PA

Audience: Industry, Government, Academia

Format: Workshop

Registration:

https://www-s.nist.gov/CRS/conf_disclosure.cfm?conf_id=6269

Registration Contact:

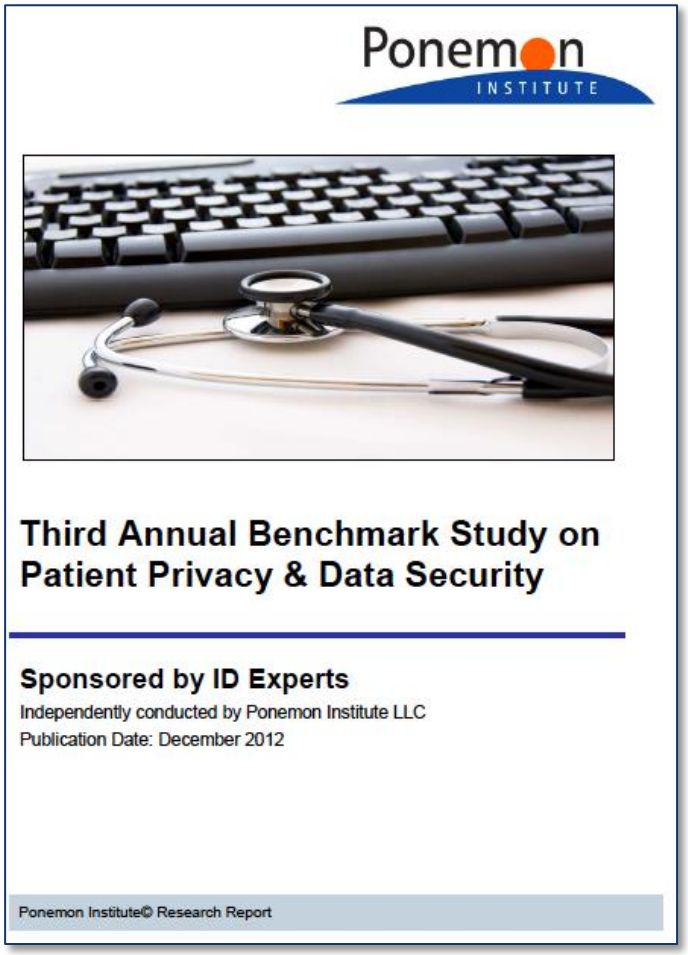
Angela Ellis

angela.ellis@nist.gov

Healthcare & Public Health Demographics

(Approximate)

Healthcare Personnel (13,000,000)	Hospitals (5000+)
Pharmacies (70,000)	Pharmaceutical Manufacturers (2,500+)
Biotech Companies (1000)	Medical Manufacturers/Distributors (1500)
Health Departments (3000)	Home Health Agencies (7000)
Long-term Care Facilities (70,000)	Ambulatory Facilities (300,000)
Health-related Labs (170,000)	Biotech Companies (1000)
Health Insurers & Payers (1000)	Funeral Homes (20,000)



Average data breach impact - $ 2.4 Million

Average cost to healthcare industry….

$ 7 BILLLION

Of the Healthcare Organizations Surveyed….

94% - Data Breach in Last Two Years

81% Permit Employees / Medical Staff To:

Utilize Own Mobile Devices (BYOD

Connect to Networks / Enterprise Systems

The Washington Post

Year Long Cybersecurity Examination

Dec. 2012

- **Healthcare Sector Most Vulnerable Industry**

Lags behind, not addressing security

Ignoring known flaws in aging technology

Culture - Sidestepping basic security measures for convenience

Washington Post Study - Perpetrators

"I have never seen an industry with more gaping security holes," said Avi Rubin, a computer scientist and technical director of the Information Security Institute at Johns Hopkins University.

"If our financial industry regarded security the way the health-care sector does, I would stuff my cash in a mattress under my bed."

The Washington Post By Robert O'Harrow Jr,December 25, 2012

- **Hacktivists / Cyber warriors**
- **Bad Actors / Criminals**
- **State Sponsored – Nation States**
- **Terrorists**
- **Internal – Intentional**
- **Internal - Unintentional**

Personal Health Information

- Financially attractive to criminal element as the street value is worth fifty times that of personal information

(Source: http://www.claimsjournal.com/news/national/2012/06/14/208510.htm)

- Health care data breaches are on the rise, with one in every six attacks in 2009 aimed at health care

(Source: http://www.rsa.com/products/consumer/whitepapers/11030_CYBHC_WP_0710.pdf)

- Resulting harm includes theft of: personal financial information which can result in identity theft; medical identity theft which can result in denial of medical coverage; medical record alteration which can result in misdiagnosis, improper treatment and ultimately death

(Source: http://promos.mcafee.com/en-US/PDF/idtheft_eguide_us.pdf)

Medical Devices

- Ethical hacks of medical devices, including insulin pumps and pacemakers, have received a great deal of media attention

- Medical device security breaches could result in patient harm even death and expose companies to potential blackmail attempts

(Source: http://www.databreachtoday.com/fda-tackling-medical-device-security-a-5210)

- Currently an effective reporting mechanism for medical device security threats from industry to government does not exist

(Source: http://www.redorbit.com/news/science/1112660479/medical-device-cybersecurity-needs-better-systems/)

Search Engine Danger

Runs 24/7 – Collecting location and device data for 500 million devices …….and growing

Intellectual Property

- Statistics on the occurrence of intellectual property theft are difficult to produce as companies do not want to publicize the breaches or bring attention to vulnerabilities

(Source: https://www.mckinseyquarterly.com/PDFDownload.aspx?ar=2821)

- Estimates of the economic cost to business attributable to IP theft range from $200 billion to $250 billion and cost 750,000 jobs

(Source: http://www.nw3c.org/docs/whitepapers/intellectual_property_theft_september_201008B6297ECEB4FAE7EAA79494.pdf?sfvrsn=3)

- Bio, pharma and medical device manufacturers are all targets for IP theft which increasingly occurs through cyber attacks

World Privacy Forum 2013

Street Cost – Social Security Number……..$ 1

Street Cost – Financial Record …….. .50

Street Cost – Medical Record …….. $ 50

- Lawsuits
- Criminal Charges
- Regulatory Compliance Actions
- Fines
- Damage to Reputation / Image
- Loss of Public Trust/Confidence

- **Life !**
- **Organizational Operational Integrity**
- **Business & Financial Systems**
- **Data**
- **Medical Devices & Device Corruption**
- **Environmental Systems**
- **Facilities**
- **Medical Insurance / Identity / Coverage**

National Health ISAC (NH-ISAC)

NH-ISAC

Nation's Healthcare & Public Health Critical Infrastructure Recognized ISAC

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)

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 Headquarters

Global Institute for Cybersecurity + Research
Global Situational Awareness Center (GSAC)
NASA / Kennedy Space Center
Space Life Sciences Laboratory

NASA – Technology Education Center
Cybersecurity Intelligence, Research & Education
Astronaut Memorial Foundation

Objective: Understanding Of..

NH-ISAC Capabilities

- 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
- Sector and Cross-Sector Analysis / Two-Way Information Sharing / Incident Response
- Early Notifications / Alerts – Actionable Intelligence
- National Healthcare & Public Health Cybersecurity Exercises
- Cyber and All-Hazards Event Resiliency Support / Response
- Security Risk Management / Leading Practice
- Awareness / Workforce Education

NH-ISAC Capabilities

NH-ISAC provides:

- **Delivery of timely, relevant and actionable alerts from various sources distributed through the NH-ISAC Situational Awareness Center;**
- **Trusted mechanisms to facilitate member sharing of threat, vulnerability and incident information, in either an attributed or non-attributed manner;**
- **Sector-specific groups and subcommittees that provide forums for members in a given part of the sector;**
- **Bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;**
- **Engagement with private security companies to identify threat information of relevance to the membership and the sector;**
- **Development of risk mitigation best practices, threat viewpoints and toolkits, as well as member-driven research regarding best practices at member organizations through the Leading Practice Committee.**

US DHS – Formal Collaboration

US Department of Homeland Security

DHS National Protection and Programs Directorate (NPPD)

Office of Infrastructure Protection (IP)

Lead National Program to Reduce CI/KR Risks

Strengthen National Preparedness, Response and Rapid Recovery

Office of Cybersecurity & Communications

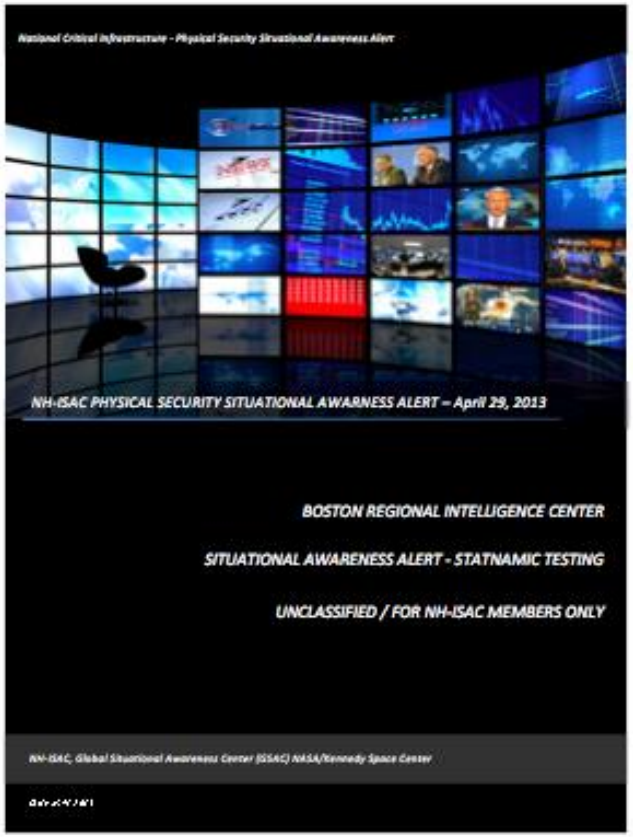
National Cybersecurity Division (NCSD) - Cyber Exercises, National Cybersecurity Education

US CERT - Improve, Manage, Coordinate Information Sharing

National Cybersecurity & Communications Integration Center (NCCIC)

Government (Fed, State, Local), Intelligence and Law Enforcement Communities, Private Sector

Alerts / Advisories / Reports



NATIONAL HEALTHCARE & PUBLIC HEALTH SECURITY INTELLIGENC

INFORMATION SHARING

LOCKHEED MARTIN

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,

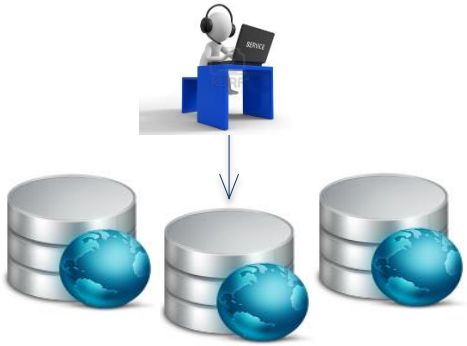
NH-ISAC Analyst
US DHS – NCCIC

NH-ISAC
Security Analysts
Intelligence Analysis

NH-ISAC
Internal Security Intelligence
Threat + Vulnerability
Analysis, Export/Import
Management

Members' Trusted
Threat Information Sharing Portal

NH-ISAC
Member Community



NH-ISAC Members' CMS Security Intelligence Feeds

National Healthcare & Public Health Cybersecurity Response System

Security Situational Awareness & Information Sharing

All-Hazards (Physical/Cyber) Security Intelligence, Actionable Intelligence

Sector/Cross-Sector Analysis, Reporting, Information Sharing

National Healthcare & Public Health Cybersecurity Response System (HPH-CRS)

National HPH Security Intelligence (HPH-SI)

Situational Awareness, Actionable Intelligence

Two-Way Information Sharing

Countermeasure Solutions / Incident Response

National HPH Cybersecurity First Responder (HPH-CFR)

Organizational, Sector, Cross-Sector, State / Federal Government

Annual Training / Certification

National HPH Cybersecurity Education Framework (HPH-CEF)

Health Sector Role-Based Cybersecurity Education / Certifications

National Healthcare & Public Health Cybersecurity Council

NATIONAL HEALTHCARE & PUBLIC HEALTH CYBERSECURITY COUNCIL

STATE-SPECIFIC COUNCILS

INITIAL WEBINAR / STATE-WIDE WORKSHOP

DEFINE PROTOCOLS

CYBER RESPONSE – ALL-HAZARDS - MAPPING TO PHYSICAL RESPONSE

CYBER INTELLIGENCE & INFORMATION SHARING

CYBER FIRST RESPONDERS - ORGANIZATIONAL/SECTOR/CROSS-SECTOR/GOV

CYBERSECURITY AWARENESS & WORKFORCE EDUCATION

Cyber Response Communications Command & Control

Collabria

ReadyOp

- **Planning, Managing, Communicating and Directing Activities – Unified Command Structure**
- **Nationwide Visual Database of Healthcare and Public Health Emergency Contacts – CYBER FIRST RESPONDERS**
- **Instance Nationwide Communications & Exercises**
  - **Cell Phone**
  - **Text**
  - **Email**
  - **Secure Voice**
  - **Radio**

Why Engage ?

- ***Success Relies on Private Sector Engagement***
- **Failure Is Not an Option**

At the end of the day, your Organization's economic health and well-being are at stake

Your Opportunity to Engage…

YOUR OPPORTUNITY TO ENGAGE WITH A DEFINING VOICE IS NOW!

National Health ISAC (NH-ISAC)

Global Institute for Cybersecurity + Research

Global Situational Awareness Center

NASA/ Kennedy Space Center

Deborah Kobza, Executive Director / CEO

dkobza@nhisac.org, 904-476-7858