Cybersecurity Resilience

Securing the Infrastructures that Secure Healthcare & Public Health
National Level - Critical Infrastructure Cybersecurity Resilience

National Information Sharing & Analysis (ISAC) Infrastructure

National Health ISAC (NH-ISAC)

Global Cyber Range (CGR)
“Systems and Assets, Whether Physical or Virtual So Vital to the United States That the Incapacity or Destruction of Such Systems and Assets Would Have a Debilitating Impact On Security, National Economic Security, National Public Health or Safety”

Close to 90% of the Nation’s Critical Infrastructures Are Owned and Operated By the Private Sector
### Sector-Specific Agency (SSA) vs. Critical Infrastructures & Key Resources

<table>
<thead>
<tr>
<th>SSA</th>
<th>Critical Infrastructures &amp; Key Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department Of Agriculture</td>
<td>Agriculture &amp; Food</td>
</tr>
<tr>
<td>Department of Health &amp; Human Services</td>
<td>Healthcare &amp; Public Health</td>
</tr>
<tr>
<td>Department of Defense</td>
<td>Defense Industrial Base</td>
</tr>
<tr>
<td>Department of Energy</td>
<td>Energy</td>
</tr>
<tr>
<td>Department of the Interior</td>
<td>National Monuments and Icons</td>
</tr>
<tr>
<td>Department of the Treasury</td>
<td>Banking &amp; Finance</td>
</tr>
<tr>
<td>Environmental Protection Agency</td>
<td>Water</td>
</tr>
<tr>
<td>DHS Office of Cybersecurity &amp; Communications</td>
<td>Information Technology Communications</td>
</tr>
<tr>
<td>DHS Transportation Security Administration</td>
<td>Postal and Shipping</td>
</tr>
<tr>
<td>DHS Transportation Security Administration United States Coast Guard</td>
<td>Transportation Systems</td>
</tr>
<tr>
<td>DHS Immigration &amp; Customs Enforcement, Federal Protective Service</td>
<td>Government Facilities</td>
</tr>
</tbody>
</table>

---

**Presidential Directive**

**Identify, Prioritize, Protect**

**National Critical Infrastructures & Key Resources (CI/KR)**

**National Infrastructure Protection Plan (NIPP)**

**Protection Efforts and Resiliency**

**Sector-Specific Agencies (SSAs) + Plans**

**Information Sharing & Analysis Centers (ISACs)**
Managing Risks from Significant Threats and Hazards to Physical and Cyber Critical Infrastructures

Requires an Integrated Approach Across a Trusted Diverse Community

Identify, Deter, Detect, Disrupt and Prepare for Threats and Hazards

Reduce Vulnerabilities of Critical Assets, Systems and Networks

Mitigate the Potential Consequences to Critical Infrastructure of Incidents or Adverse Events
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.

Formed in Response to a Presidential Directive

Private-Sector Led

Nationally Recognized

Federal Sector-Specific Agency (SSA)

Sector’s Coordinating Council (SCC)

Intelligence Agencies (DHS, FBI, NSA)

National Council of ISACs

Critical Infrastructure Owners and Operators.
Official Public/Private Critical Infrastructure Resilience Infrastructure – Collective Action

- US Dept. Homeland Security
- Federal Sector-Specific Agencies (SSA)
- Coordinating Councils (SCC)
  - Government Coordinating Council (GCC)
  - (Private) Sector Coordinating Council (SCC)
- Information Sharing & Analysis Centers (ISACs)
- Cross-Sector Cybersecurity Working Group
- Unified Cyber Coordination Group
- Federal Senior Leadership Council (FSLC)
- State/Local/Tribal/Territorial (SLTTGCC)
- Regional Consortium Coordinating Council (RC3)

Presidential Policy Directive
PPD-21
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)
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.

For Immediate Release

February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY
Executive Order 13636 – Improving Critical Infrastructure Cybersecurity

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014
Framework Core

Identify | Protect | Detect | Respond | Recover

Identify (Systems, Assets, Data, Capabilities)
Protect (Develop and Implement Safeguards)
Detect (Timely Discovery of Cybersecurity Events)
Respond (Develop and Implement Appropriate Action Activities)
Recover (Develop and Implement Resilience Plans – Restore Capabilities)

**Information Sharing & Analysis Centers (ISACs)**

The Framework encourages leveraging guidance and trusted security situational awareness intelligence and information sharing mechanisms from the nation’s ISAC infrastructure to achieve broader cybersecurity situational awareness intelligence for effective response.
Framework Profile

Alignment of Functions, Categories and Subcategories

with

Business Requirements, Risk Tolerance and Organization Resources

Establishes Reducing Cybersecurity Risk

Current Profile | Target Profile

Current Profile – Cybersecurity Outcomes Currently Being Achieved
Target Profile – Outcomes Needed to Achieve Cyber Risk Management Goals

Profile Comparison

Gap Mitigation Cost-Effective Roadmap
Public Workshop - Collaborative Approaches for Medical Device and Healthcare Cybersecurity, October 21-22, 2014

In recognition of National Cybersecurity Awareness Month, the Food and Drug Administration (FDA) in collaboration with the Department of Health and Human Services (HHS) and the Department of Homeland Security (DHS) is announcing a public workshop “Collaborative Approaches for Medical Device and Healthcare Cybersecurity.”

This workshop will bring together all stakeholders in the healthcare and public health (HPH) Sector including but not limited to medical device manufacturers, healthcare facilities and personnel (e.g., healthcare providers, biomedical engineers, IT system administrators), professional and trade organizations (including medical device cybersecurity consortia), insurance providers, cybersecurity researchers, local, State and Federal Governments, and information security firms in order to identify HPH cybersecurity challenges and ways the Sector can work together to address these challenges.
HEALTHCARE PROVIDER CYBERSECURITY FRAMEWORK

HEALTHCARE PROVIDER CYBER RESILIENCE REVIEW

NATIONAL HEALTH CYBERSECURITY RESILIENCE

REGIONAL ROUNDTABLES

Atlanta | Boston
Chicago | Dallas
Seattle
San Francisco (Dec. 3 & 4)
MEMORANDUM OF UNDERSTANDING
BETWEEN THE NATIONAL HEALTH INFORMATION SHARING & ANALYSIS CENTER, INC. (NH-ISAC)
AND THE U.S. FOOD AND DRUG ADMINISTRATION CENTER FOR DEVICES AND RADILOGICAL HEALTH

I. Purpose:
The United States Food and Drug Administration (FDA)’s Center for Devices and Radiological Health (CDRH) and The National Health Information Sharing & Analysis Center, Inc. (NH-ISAC) have a shared interest in encouraging the identification, mitigation, and prevention of cybersecurity threats to medical devices. Both FDA and NH-ISAC are referred to individually as a “Party” and collectively as the “Parties.” This Memorandum of Understanding (MOU) establishes the terms for collaboration to promote this shared interest.

II. Background:
1. FDA is authorized to enforce the Federal Food, Drug, and Cosmetic Act (“the Act”) as amended (21 U.S.C. 301). In fulfilling its responsibilities under the Act, FDA among other things, directs its activities toward promoting and protecting the public health by ensuring the safety, efficacy, and security of drugs, biological products, veterinary products, medical devices and radiological products and the safety and security of foods.
Proactive Collaboration Goals

Create an environment fostering stakeholder collaboration and communication and encouraging sharing medical device cybersecurity vulnerabilities and the security of surrounding healthcare IT.

Develop awareness of the Volunteer Cyber Framework, operationalize for successfully adoption for organizations and products.

Encourage HPH stakeholders to develop innovative strategies to access and mitigate cyber vulnerabilities that affect their products.

Build foundation of trust within the HPH community

Benefit from cybersecurity threat and vulnerability information sharing

Leverage intelligence feeds from other sectors

Timely situational awareness of vulnerabilities and negative consequences for patient safety – share solutions
Agreement

FDA – Establish a mechanism by which cybersecurity vulnerabilities + threats can be shared with NH-ISAC.

NO CONFIDENTIAL, COMMERCIAL, TRADE SECRET OR PERSONAL PRIVACY INFORMATION

NH-ISAC – Work with members to establish a mechanism by which medical device cybersecurity vulnerabilities are shared with the FDA

FDA + NH-ISAC – Work together to establish how stakeholders can interface with the FDA (medical device or healthcare cybersecurity vulnerability information sharing)

Collaboration – Inform a risk threshold common understanding upon which exploits of a vulnerability might impact patient safety and/or public health.

Develop a shared understanding of risks posed by medical device cyber vulnerabilities.

Foster development of a shared risk assessment framework to enable stakeholders to consistently and efficiently assess patient safety, address risks and take appropriate mitigation actions.
NH-ISAC

Nation’s Healthcare & Public Health Critical Infrastructure - Official ISAC

National Council of ISACs

Health Sector Coordinating Council (GCC/SCC) Executive Committee

SCC Chair, Cybersecurity Legislation

Appointed by HHS - DHS Cyber Unified Coordination Group (UCG)

Representation - DHS National Critical Infrastructure Protection Advisory Council (CIPAC)

NH-ISAC MISSION

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

• Trusted Security Actionable Intelligence

• Sector and Cross-Sector Analysis

• Early Warnings, Notifications (Physical + Cyber)

• Countermeasure Solutions / Incident Response

• Fostering the Availability of Proven Security Leading Practice
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
US DHS / Office of Cybersecurity + Communications

Cooperative Research and Development Agreement (CRADA)

13-NPPD-008

“This CRADA Agreement is entered into by and between National Health ISAC (hereinafter referred to as NH-ISAC) and the United States of America, as represented by the National Protection and Programs Directorate (NPPD) Office of Cyber Security and Communications, recognized as a Federal cybersecurity and communications laboratory entity within the Department of Homeland Security

The key objective of this Agreement is to enable DHS and NH-ISAC to share cybersecurity, communications reliability and related data and information, conduct analytical collaboration activities and share technical capabilities associated with joint research, development, test and evaluation efforts associated with the security of critical infrastructure networks and systems.”
Global Situational Awareness Center (GSAC)

Cybersecurity Intelligence, Research and Education Center
One Organization’s Incident is Everyone’s Defense

Trusted Information Sharing Supports

Collaborative Analysis

Detecting Sector-Specific and Organization-Specific Targeting

Identifying new Techniques, Tactics and Procedures (TTP)

Information Sharing Issues and Challenges

Today Many Organizations Process Little of the Intelligence Received

Wide Variety of Reporting Sources -
Open Source, Proprietary/Commercial, Government, and Various Formats (Emails, Web Pages, Documents, Datafeed, Physical Meetings)

No Automated Infrastructure for Comprehensive Multisource Sharing

Volume of Information Rapidly Outgrowing Ability for Analysts to Process.
On average, it takes 7 man-hours to manually process a single threat intelligence report through all internal analysis and response actions. As a consequence only a fraction of the reports containing actionable intelligence are ever processed.
Increasing Cyber Risks

- Malicious actors have become much more sophisticated & money driven.
- Losses to US companies now in the tens of millions; WW hundreds of millions.
- Cyber Risks are now ranked #3 overall corporate risk on Lloyd’s 2013 Risk Index.

We are Solving the Problem

- Security standards recently matured.
- ISAC’s are the trusted source for sharing industry threat intelligence.
- Cyber Intelligence Sharing Platform revolutionizing sharing and utilization of threat intelligence.

Yesterday’s Security

Network Awareness
Protect the perimeter and patch the holes to keep out threats and share knowledge internally only.

Today’s Problem

Intelligence Sharing
Identify and track threats, incorporate knowledge and share what you know manually to trusted others. Extremely time consuming and ineffective in raising the costs to the attackers.

Manually Sharing Ineffective

- Expensive because it is slow manual process between people.
- Not all cyber intelligence is processed; probably less than 2% overall = high risk.
- No way to enforce cyber intelligence sharing policy = non-compliance.

Tomorrow’s Solution

Situational Awareness
Automate Sharing
Develop clearer picture from all observers’ input and pro-actively mitigate.
**STIX - 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

**TAXII**

Trusted Automated eXchange of Indicator Information
NATIONAL HEALTHCARE & PUBLIC HEALTH CYBERSECURITY RESILIENCE

Cybersecurity Situational Awareness Intelligence Information Sharing and Coordinated National Response

Global Security Intelligence and Technology Partners
National Council of ISACs (Sector/Cross Sector Intelligence)
Government Collaborative Security Intelligence

US DHS, HHS, Government Partners

Trusted Intelligence Partners

NH-ISAC Security Intelligence Repository

Other ISACs NCI Directorate

Manual Intelligence Information Sharing

NH-ISAC Members

Automated Intelligence Information Sharing

STIX/TAXII Compliant
STIX Cyber Constructs
TAXII Transmission
Automated Intelligence Information Sharing

National Health ISAC (NH-ISAC)
Global Situational Awareness Center
Global Institute for Cybersecurity + Research
NASA/Kennedy Space Center
National Health Cybersecurity Intelligence Information Sharing (NH-CIIS)
All-Hazards (Physical/Cyber) Security Actionable Intelligence
Sector/Cross-Sector Analysis, Reporting, Two-Way Information Sharing

NH-ISAC Cybersecurity Threat Intelligence Repository
Automated Situational Awareness Actionable Intelligence
Two-Way Information Sharing

National Health Cybersecurity Communications and Control
Secure Unified Communications and Control Platform
Planning, Managing, Exercising, Coordination, Directing
Instant Communications
Cell / Landline / Text / Email / Secure Voice / Secure Video / Radio
NH-ISAC ReadyOp

- Planning, Managing, Communicating and Directing Activities – Unified Command Structure
- Nationwide Visual Database of Healthcare and Public Health Security Stakeholders
- Instant Nationwide Communications
  - Cell Phone
  - Text
  - Email
  - Secure Voice / Secure Video
  - Radio
ReadyOp

- Alerts
- Event News/Updates
- Immediate Actions
- Instructions
- Response Updates
- Maps
- Requests

Secure Communications
- Voice
- Text
- Email

- Rosters / Assets
- Emergency Meetings
- Equipment Requests
- Support Needed
- Support Available
- Pictures

33 - (NH-ISAC) National Healthcare & Public Health Cybersecurity Resilience
Cybersecurity Resilience – A Three-Tiered Approach

NIST Framework for Improving Critical Infrastructure Cybersecurity

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Global Cyber Range

34 - (NH-ISAC) National Healthcare & Public Health Cybersecurity Resilience
On-Demand 24/7 LIVE Cyber Range Professional Development Environment
Access Anywhere with an Internet Connection & Web Browser – No Plug-Ins, No Software
Dynamically Access a Host of Virtual Machines - Preconfigured with Vulnerabilities, Exploits, Tools and Scripts
Target Machines – Completely Virtualized - Customizable to Simulate Enterprise Networks
100% Control of the Environment

NASA Center for Lifecycle Design – Modeling & Simulation
Secure Design Integration, Cyber Exercise Scenarios
CYBER FIRST RESPONDER (CFR)

ALIGNMENT OF

CYBER + PHYSICAL RESPONSE PROTOCOLS = ALL HAZARDS

(Organizational, Sector, Cross-Sector, Government)

Education | Certification
National Initiative for Cybersecurity Education
The Framework establishes:

- A common taxonomy and lexicon which organizes cybersecurity into 31 specialty areas within 7 categories.
- A baseline of tasks, specialty areas, and knowledge, skills and abilities (KSAs) associated with cybersecurity professionals.

The Framework assists with strategic human capital efforts, including:

- Workforce Planning
- Recruitment and Selection
- Training and Development
- Succession Planning
Framework Categories and Specialty Areas

- The Framework's 31 Specialty Areas (SA), organized into 7 Categories, encompass the entirety of national cybersecurity work.

- Organizations can use the SAs to identify, build, and customize cybersecurity roles based on mission requirements.

This is the tie to the OPM Data Element and EHRI.
Welcome to the Global Cyber Range (GCR)

Are you a new user? Create an account to register your access code and get started. Make sure you have your access code handy before registering!

Already have an account with GICSR's National Cyber Range? Simply log into your existing account to register a new access code or begin a new session.
Cloud-Based | 100% Automated “ 100% Virtualization
Accessible Anywhere – Via Internet Connection
Instant Connectivity to all Range Labs

Access to Real-World Tools and Scenarios
After Log-In – Full Access to Preconfigured Targets, Networks and Attack Tools

Preconfigured Vulnerable Websites | Hidden Victim Machines
Vulnerable, Unpatched Operating Systems
Fully Networked Environments
Forensic Cast Files and Hard Disks
Planning

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

Public/Private Proactive Response | Critical Functions Resiliency

Forming Partnerships

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/ Kennedy Space Center
Deborah Kobza, Executive Director / CEO
dkobza@nhisac.org, 904-476-7858