The Office of the National Coordinator for Health Information Technology

# Information Sharing and Analysis Organization (ISAO) Initiative Update

## Health IT Joint Committee Collaboration Briefing

Rose-Marie O. Nsahlai, Office of the Chief Privacy Officer, ONC
Nickol Todd, Assistant Secretary for Preparedness and Response (ASPR)

October 5, 2016

# Agenda

- Welcome & Introductions
- Background and Overview
  - Purpose of the ISAO Initiative
  - Expected Outcomes
  - Current State-ASPR Planning Award
- Awardee Information
- Wrap up

# Background

- Section 3001(b) of the HITECH Act established ONC, in part, to support the development of a nationwide health information technology infrastructure.
- One of ONC's guiding principles for nationwide interoperability in the health IT infrastructure is to "protect privacy and security in all aspects of interoperability." (Principle #3, *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*).
- To support this guiding principle, ONC committed to "coordinate with the Office of the Assistant Secretary for Preparedness and Response (ASPR) on priority issues related to cybersecurity for critical public health infrastructure" (Commitment #C3.3).

# Background

Recent Healthcare Data Breaches

Executive Orders and Administration Priority

Nationwide Interoperability Roadmap

Federal Health IT Strategic Plan

2015 Edition Health IT Certification Rule

# Background

- As recent news reports show, security breaches and ransomware attacks in the Healthcare and Public Health sector are on the rise. Criminal cyber attacks against health care organizations are up 125 percent compared to five years ago, replacing employee negligence and lost or stolen laptops as the top cause of health care data breaches. The average consolidated total cost of a data breach was $3.8 million, a 23 percent increase from 2013 to 2015.

- To better prevent attacks on health information technology, organizations need better visibility into what to expect and how to respond. Therefore, for the past three years, ONC has worked in partnership with the Assistant Secretary for Preparedness and Response (ASPR), the Office of the Assistant Secretary for Administration (ASA),the Office of the Chief Information Officer's (OCIO) Office of Information Security (OIS), and the Office of Security and Strategic Information's (OSSI) Cyber Threat Intelligence Program (CTIP) to develop the means to facilitate cyber threat information sharing across the Healthcare and Public Health sector.

# Background

- **Cybersecurity Information Sharing Act (CISA)**
  - Outlines new requirements for cyber threat information sharing.
  - Section 405(c) of the Act establishes Health Care Industry Cybersecurity Task Force.
    - Section 405 (c) (1) (D) and 405 (c) (1) (E) outline the task force's duties regarding recommendations for cybersecurity threat information dissemination
    - Task  force asked to recommend a plan for federal Government and Health Care and Public Health (HPH) sector stakeholders to share actionable cyber threat indicators and defensive measures.

# Background

- **Executive Order (EO) 13636**, Improving Critical Infrastructure Cybersecurity (February 19, 2013), defined HHS's information sharing role with respect to cybersecurity threats.
- EO 13636 calls on HHS to participate with other Sector-Specific Agencies and the Department of Homeland Security to "increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats."

# Background

- On February 13, 2015, the President signed **Executive Order (EO) 13691**, Promoting Private Sector Cybersecurity Information Sharing.
- EO 13691 encourages the development of “information sharing and analysis organizations” (“ISAO”s) to serve as focal points for cybersecurity collaboration within the private sector and between the private sector and government.
    - This broadens existing terminology related to “information sharing and analysis centers” (“ISAC”s), by identifying ISACs as one type of organization among other types of ISAOs.

# Background: ISACs and ISAOs

| ISACs | ISAOs |
|---|---|
| Usually aligned with one or more of the 16 critical infrastructure sectors | Do not need to be organized by sector, and may instead be organized by geography, type of threat, professional affiliation, etc. |
| All ISACs are ISAOs; Due to Executive Order 13691 which aimed to expand information sharing via ISAOs | ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest |
| Collaborate with DHS with limited structure | Provide a partnership structure for DHS and the government to connect with the private sectors |
| Sector-based ISACs collaborate and coordinate with each other via the National Council of ISACs (NCI) | National Cybersecurity and Communications Integration Center (NCCIC) can enter into information sharing agreements with ISAOs for increased collaboration between ISAOs and the Federal government |

# Purpose of the Awards

- The Purpose of the ISAO Cooperative Agreement is to
  - » expand the capacity of an existing ISAO or ISAC to share cyber threat information (CTI) bi-directionally between HHS and the HPH sector; and
  - » provide outreach and education to the HPH sector on how to take action on threats identified.
- The goal is to improve cyber security awareness within the HPH sector and to equip sector stakeholders to take action in response to CTI shared by the ISAO.

# Key Details of Awards

Cooperative agreements totaling $350,000 awarded to strengthen the ability of health care and public health sector partners to respond to cybersecurity threats.

| Type of Award | ONC Cooperative Agreement | ASPR Cooperative Agreement |
|---|---|---|
| Award Amount | $250,000 | $100,000 |
| Number of Awards | 1 | 1 |
| Award Date | 9/26/2016 | 9/26/2016 |

# Overarching Goals of ONC's Award

- Provide cybersecurity information and education on cyber threats affecting the Healthcare and Public Health sector
- Expand outreach and education activities to assure that information about cybersecurity awareness is available to the entire Healthcare and Public Health sector
- Equip stakeholders to take action in response to cyber threat information
- Facilitate information sharing widely within the Healthcare and Public Health Sector, regardless of the size of the organization
- Fulfills commitment C3.3 in final Interoperability Roadmap

# ONC Award Program Objectives

It is expected that the recipient will be able to:

1. Build internal resources to serve as a single ISAO
2. Expand its current membership base;
3. Focus more of its business and resources on CTI sharing;
4. Create a lower entry cost for smaller HPH sector organizations who wish to join an ISAO; and
5. Eventually provide some level of free CTI sharing services to the entire HPH sector.

# Purpose of ASPR’s Award

- Provide resources to focus the awardee’s efforts on cybersecurity information sharing
- Broaden access to cybersecurity information for healthcare organizations of smaller sizes
- Reduce the costs to organizations receiving cyber threat information

# Overarching Goals of ASPR's Award

- Address gaps identified in the gap analysis performed under 2015-2016 planning award
- Develop a concept of operations (CONOPS) for multi-directional cybersecurity information sharing within the HPH Sector
- Expand the reach of the ISAO's communications mechanism
- Develop a business plan for ISAO sustainability and growth.
- Integrate information sharing activities into national approach
- Gather and Analyze cybersecurity information from private sector healthcare organizations to identify trends

# Who was Eligible to Apply?

- Local, public nonprofit institution/organizations, Private nonprofit institution/organization, Private and for profit organizations that are already providing outreach and technical assistance to participating organizations on cybersecurity threats.
- Organization that currently provides CTI sharing services to some parts of the HPH sector and seeks to expand the reach of those services.
- Organization that provides CTI sharing services to a sector other than HPH, and seeks to expand their services to the HPH sector.

# Findings-ISAO Planning Award

- Perceived effectiveness of cyber threat information sharing was low
- Organizations vary between potential sensitivity to price (preferring free options) and favoring more “reputable” sources
- There is generally low awareness, appreciation, and/or understanding amongst the respondents of common/popular cyber threat information sharing standards such as STIX, TAXII, and TLP
- Automation is highly preferred amongst all respondents
- 93% of respondents would like an ACTIVE ISAO that provides threat intelligence, analysis, and education ,and not simply a platform to share
- Operationalize Sharing as part of Incidence Response

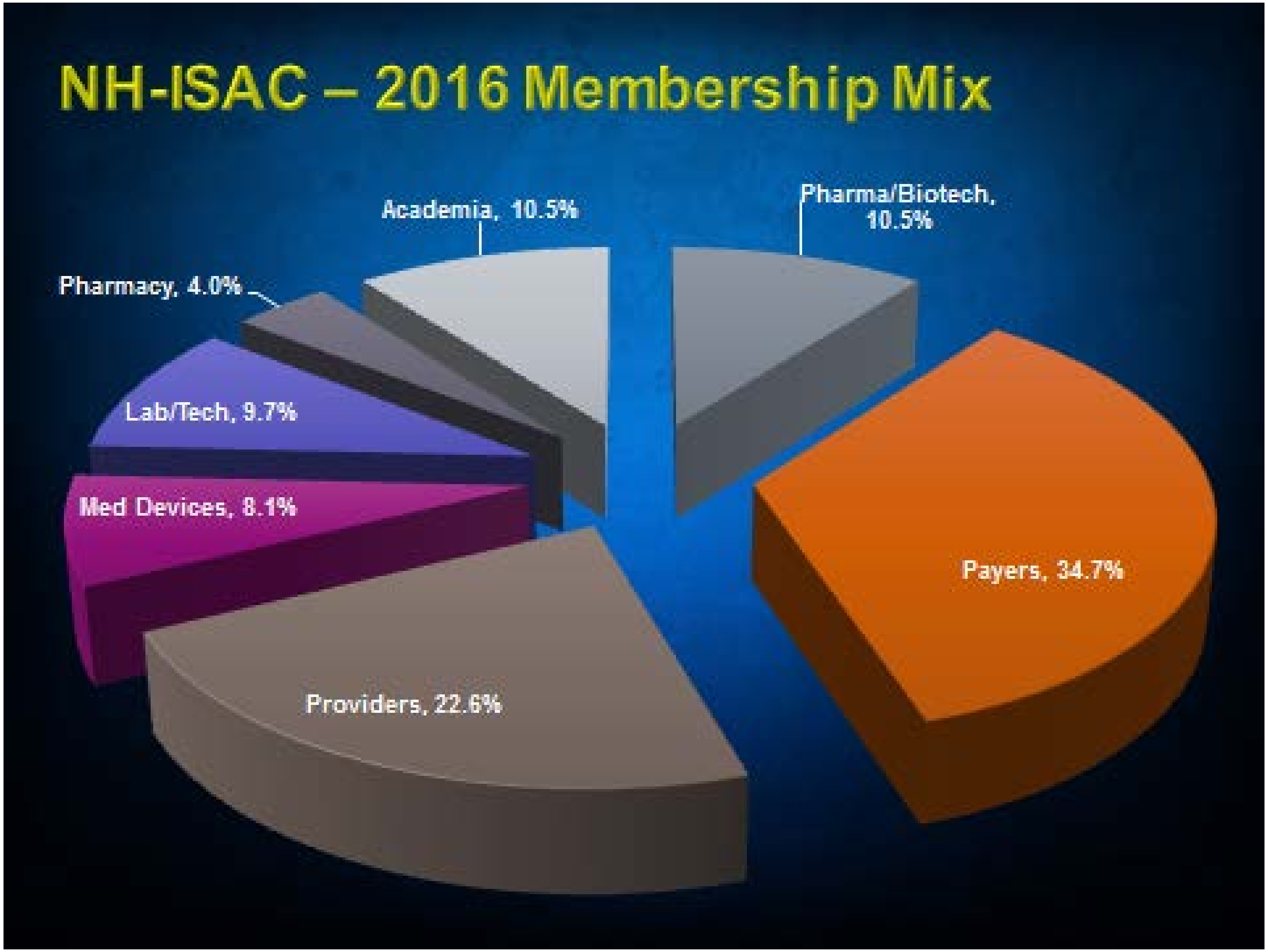
# The Grantee- NH-ISAC

National Health Information Sharing and Analysis Center (NH-ISAC)

HPH Sector Designated ISAC:

- Sharing Community
- Intelligence and Alerts
- Newsletter
- Exercises
- Webinars/Threat Calls
- Conferences & Workshops
- White Papers
- Working Groups/Committees
- Tools – Symphony, Soltra, Brightpoint
- Playbook & Threat Level
- CyberFit

# Grantee Overview-II



# Types of Information Shared

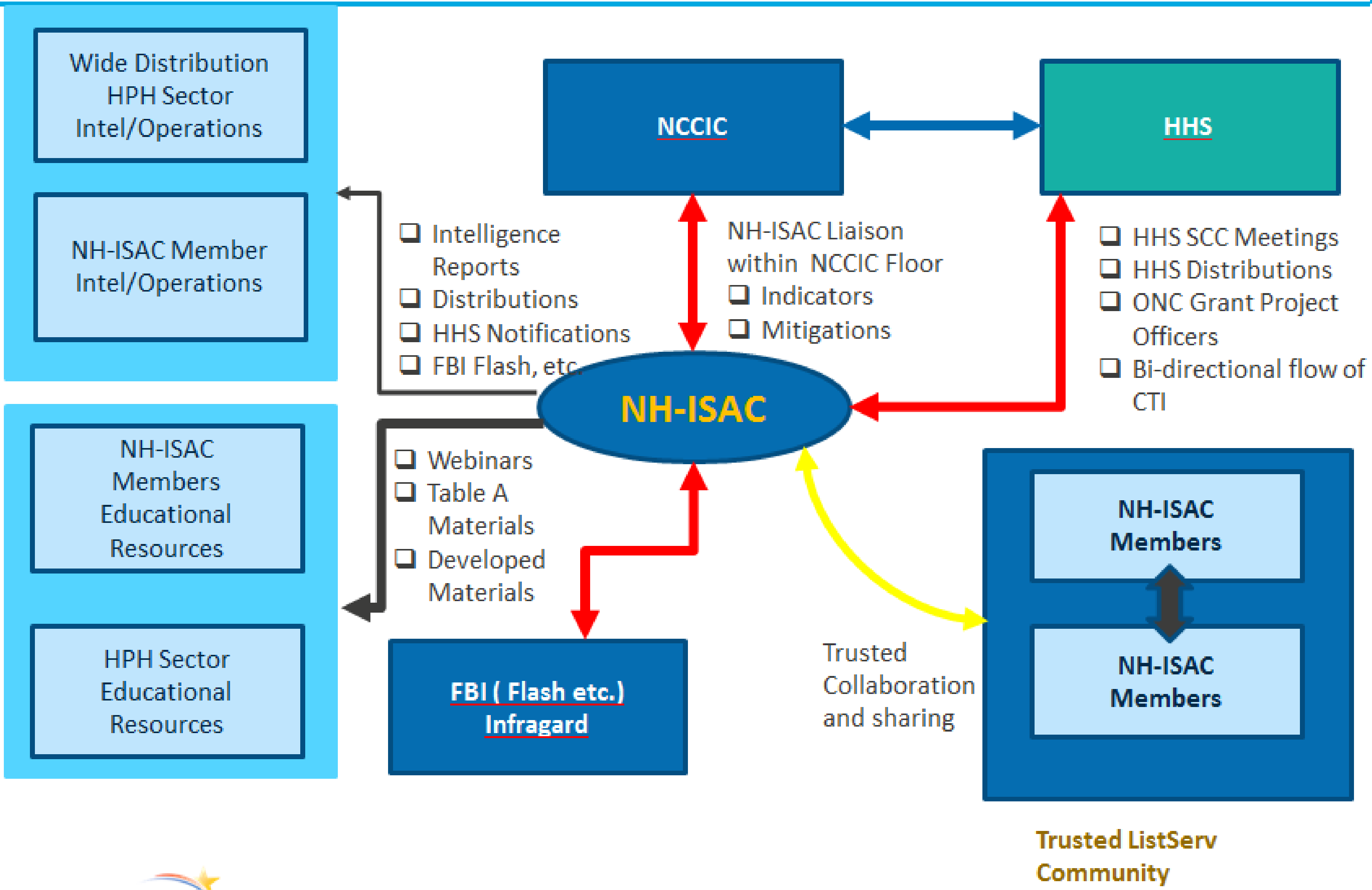
## Cyber Threats, Vulnerabilities, Incidents

- ✓ Malicious Sites
- ✓ Threat Actors, Objectives
- ✓ Threat Indicators
- ✓ TTPs, Observables
- ✓ Courses of Action
- ✓ Exploit Targets
- ✓ Denial of Service Attacks

- ✓ Malicious Emails:

  Phishing/ Spearphishing
- ✓ Software Vulnerabilities
- ✓ Malicious Software
- ✓ Analysis and risk mitigation
- ✓ Incident response

# NH-ISAC Core Sharing – Government / Private Sector


Wide Distribution HPH Sector Intel/Operations
NH-ISAC Member Intel/Operations
NCCIC
HHS
❑ Intelligence Reports
❑ Distributions
❑ HHS Notifications
❑ FBI Flash, etc.
NH-ISAC Liaison within NCCIC Floor
❑ Indicators
❑ Mitigations
❑ HHS SCC Meetings
❑ HHS Distributions
❑ ONC Grant Project Officers
❑ Bi-directional flow of CTI
NH-ISAC
NH-ISAC Members Educational Resources
HPH Sector Educational Resources
❑ Webinars
❑ Table A Materials
❑ Developed Materials
FBI ( Flash etc.) Infragard
Trusted Collaboration and sharing
NH-ISAC Members
NH-ISAC Members
Trusted ListServ Community

# Additional information

For the FAQ and additional information on this FOA, go to https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/opportunity-sharing-information-cyber-attacks/

# Wrapping It Up…Thank You!

Thank you FACA members for the opportunity to present this initiative.