Barriers & Solutions Readout Report
Version 1
Working Document

Barriers and security concerns that inhibit interoperability in federated cloud environments for information exchange in disaster response, and proposed solutions

NCOIC Cyber Security IPT
Network Centric Operations Industry Consortium

March 13, 2015

This paper has been released using the NCOIC Fast Track Review Process, and thus is not a full-consensus position from the NCOIC.

Abstract: Cybersecurity Barriers & Solutions Readout Report

Key Words: Net-Centric, Barriers, Solutions, Readout Report, Cybersecurity, Cloud

Approved for Public Release 20150313

Executive Summary

NCOIC held a workshop in October 2014 in Washington DC, to discuss the barriers and security concerns that inhibit interoperability in federated cloud environments for information exchange and coordination in disaster response and health care. This readout report summarizes those barriers and security concerns, and proposes solutions.

Top 5 Barriers

1. Lack of clear RRAs (Roles, Responsibilities, Authorities)
2. Lack of common standards & lexicon & terminology
3. Inability to share status of critical infrastructure after disaster
4. Concerns over data privacy & intellectual property rights
5. Lack of coordination between government, corporations, volunteers, NGOs, churches, etc

Recommendations to Act on These Barriers and Solutions

1. Create pattern for lexicon & terminology usage in disaster response context
2. Create pattern for interoperability between existing standards, and with emerging standards, in disaster response context
3. Create pattern for what standards, protocols, and translators to use in particular disasters (e.g. In disaster A - use standard A1 & protocol A2;
   In disaster B - use standard B1 & protocol B2, etc)
4. Create pattern for integrating crowd-sourced and geospatial cloud info/maps to show what critical infrastructure is still operational in disaster response context (hospitals, gas stations, electrical power grid, radio, internet, etc)
5. Create pattern for control and sharing intellectual property and sensitive information in disaster response context (policy, agreements, standards, handshaking, etc)
6. Create pattern for RRAs in disaster response (who does what, and how)
7. Create pattern for sharing data, jurisdiction, redaction, etc to address intellectual property, sensitive information, and classification in disaster response context

Plan For 2015 (Prioritized)

1. Collaborate with Cloud Computing & Health WGs for disaster response, focusing on RRI build-out
2. Establish cybersecurity for rapid response incubator (RRI)
3. Continue to mature the solutions to the interoperability barriers identified during 2014 Cybersecurity Workshop
4. Hold follow-on cybersecurity mini-workshops
5. Write & publish patterns based on solutions to barriers identified at October cybersecurity workshop (focus on those that help RRI the most)
6. Bring in new members to the cybersecurity IPT
7. Continue to work with East West Institute and their cybersecurity teams

TABLE OF CONTENTS

1 Introduction

1.1 Purpose of This Document

The purpose of this document is to list the barriers and security concerns that inhibit interoperability in federated cloud environments for information exchange in disaster response, as well as propose solutions to those barriers. The barriers could be due to governmental (legislative, procedural), technical, business (profitability) or cultural factors.

1.2 Workshop

NCOIC held a workshop in October 2014 in Washington DC, to discuss the barriers and security concerns that inhibit interoperability in federated cloud environments for information exchange and coordination in disaster response and health care. This readout report summarizes those barriers and security concerns, and proposes solutions.

1.2.1 Purpose of Workshop

The purpose of the workshop is to identify the barriers (governance, technical, business, culture) that are prohibiting proper deployment of a Cyber environment in cross domain interoperability. NCOIC members and guests will discuss these barriers and security concerns that inhibit interoperability in federated cloud environments for information exchange and coordination in disaster response and health care.

1.2.2 Theme of Workshop

The theme of the workshop was Cybersecurity for Federated Cloud Environments as it relates to healthcare and disaster response domains

1.2.3 Output of Workshop

This readout report containing the barriers/challenges/opportunities is the output of the workshop. It is a product of the shared insights and observations from the workshop, documenting the problems, solutions and opportunities associated with developing and maintaining a secure cloud environment for rapid response situations such as natural disasters, epidemics and other crises.

1.2.4 Guest Speakers at Workshop

The following guest speakers presented at the workshop

- Dr Craig Lee of Aerospace Corp spoke on “Disaster Response through On-Demand Resource Federation”.
- Elysa Jones of Secure Exchange Technology Innovation and OASIS Emergency Mgmt spoke on “Standards, Goals, Gaps & Needs”
- Chris Thompson of Humanity Road spoke on “Digital Disaster Response”
- Dr Tom Cellucci of Cellucci Associates (Past DHS Director of R&D and Chief Commercialization Officer of US Govt) spoke on “Public-Private Partnerships to

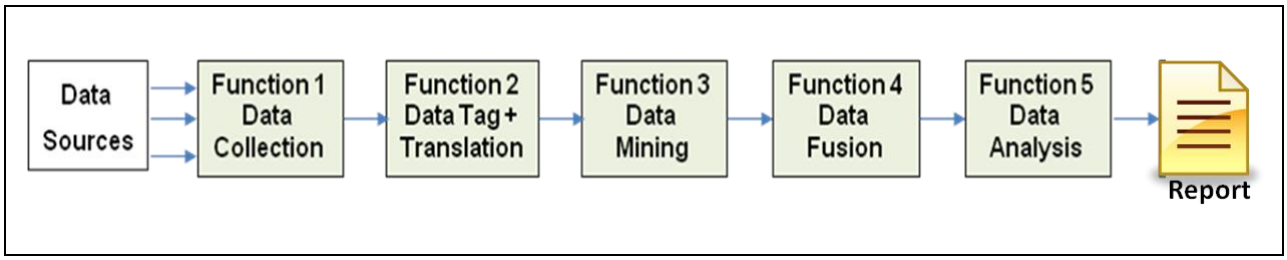
Enable Rapid Deployment of Security Capabilities"

- Bob Henley of Private Digital Network Services (PDNS) spoke on "Secure Healthcare Network System in the Cloud"

1.3 Methodology for Identifying Barriers and Solutions

We followed a classic paradigm of data collection, data mining, data fusion, data analysis, and data presentation.

- Data Collection. We collected ideas during the workshop in the form of hand-written forms, electronically submitted forms, presentations, comments made via Fuze chat session, presentations, and spoken during meeting (captured via audio/video recording).
- Data Mining. We filtered all data, and selected only those ideas that were barriers or related solutions
- Data Tagging. We assigned metadata on the ideas (barriers & sources) based on context, and were able to sort them into 4 categories (technical, business, culture, governance).
- Data Fusion. We used metadata to integrate similar barriers into single barrier, similar solutions into single solution
- Data analysis. We correlated a barrier to one or more solutions, and prioritized barriers/solutions
- Data presentation. We created a readout report document



Methodology for Identifying Barriers and Solutions

2. Barriers and Solutions

2.1 Types of Barriers

NCOIC has identified 4 types of barriers (governance, technical, business, culture), as part of the NCOIC QuadTrangle.

2.1.1 Governance Barriers

Governance Barriers are those barriers imposed by laws and legal regulations which inhibit interoperability in federated cloud environments for information exchange in disaster response.

2.1.2 Technical Barriers

Technical Barriers are those barriers due to lack of standards or poorly integrated systems which inhibit interoperability in federated cloud environments for information exchange in disaster response.

2.1.3 Business Barriers

Business Barriers are those barriers due to challenges in establishing a business case or concerns of business benefit vs. risk, which inhibit interoperability in federated cloud environments for information exchange in disaster response. These must be viewed from both the buyer and vendor perspective and so must include both profitability and affordability.

2.1.4 Cultural Barriers

Cultural Barriers are those barriers due to challenges in personnel adopting new standards, new protocols, or hesitation to work with other organizations, which inhibit interoperability in federated cloud environments for information exchange in disaster response. This could be manifested between people from different countries (e.g. crisis that occurs over international borders, or multinational response with aid workers from different countries), people from different cultural backgrounds (e.g. different religions, languages, historical enemies), different

work backgrounds (e.g. police distrust of sharing sensitive data with the general public, union workers refusing to work with non-union workers), or persons refusing to use new or untested equipment (commonly called "not invented here") or to adopt new processes or protocols (commonly called "that's not the way we do it here").

2.2 Prioritization of Barriers

All barriers were listed, and similar barriers were integrated into a single barrier category. There were over 140 barriers identified, and the 5 largest categories were selected as the "top 5" barriers.

2.3. Solutions

NCOIC identified dozens of solutions to barriers. These solutions were correlated to the barriers, such that there were numerous solutions correlated to each of the top 5 barriers.

2.4 Top 5 Barriers Identified

The top 5 barriers and security concerns that inhibit interoperability in federated cloud environments for information exchange and coordination in disaster response and health care are:

- Lack of clear RRAs (Roles, Responsibilities, Authorities)
- Lack of common standards & lexicon & terminology
- Inability to share status of critical infrastructure after disaster
- Concerns over data privacy & intellectual property rights
- Lack of coordination between government, corporations, volunteers, NGOs, churches, etc

3. Recommendations

It is recommended that the following 7 patterns be written to utilize the solutions related to these barriers. Those patterns helping the RRI will have highest priority.

1. Create pattern for lexicon & terminology usage in disaster response context
2. Create pattern for interoperability between existing standards, and with emerging standards, in disaster response context
3. Create pattern for what standards, protocols, and translators to use in particular disasters (e.g. In disaster A - use standard A1 & protocol A2; In disaster B - use standard B1 & protocol B2, etc)
4. Create pattern for integrating crowd-sourced and geospatial cloud info/maps to show what critical infrastructure is still operational in disaster response context (hospitals, gas stations, electrical power grid, radio, internet, etc)
5. Create pattern for control and sharing intellectual property and sensitive information in disaster response context (policy, agreements, standards, handshaking, etc)
6. Create pattern for RRAs in disaster response (who does what, and how)
7. Create pattern for sharing data, jurisdiction, redaction, etc to address intellectual property, sensitive information, and classification in disaster response context

4. Plan Forward for 2015

1. Collaborate with Cloud Computing & Health WGs for disaster response, focusing on RRI build-out
2. Establish cybersecurity for rapid response incubator (RRI)
3. Continue to mature the solutions to the interoperability barriers identified during 2014 Cybersecurity Workshop
4. Hold follow-on cybersecurity mini-workshops
5. Write & publish patterns based on solutions to barriers identified at October cybersecurity workshop (focus on those that help RRI the most)
6. Bring in new members to the cybersecurity IPT
7. Continue to work with East West Institute and their cybersecurity teams

5. Summary

Attendees at the NCOIC cybersecurity workshop identified 140 barriers and security concerns that inhibit interoperability in federated cloud environments for information exchange and coordination in disaster response and health care. This readout report summarizes those barriers and security concerns, and proposes solutions. The plan for next year includes writing and publishing patterns based on the proposed solutions to the top 5 barriers.

Appendix A. Presentations from Guest Speakers at Cybersecurity Workshop

Topic	Speakers	Role
Introductions and Welcome	Mark Bowler	NCOIC Tech Council Chair
NCOIC Overview	Tip Slater	NCOIC Operations Director
Plans for the Day	Andy Born	Cybersecurity IPT Chair
Disaster Response through On-Demand Resource Federation	Dr. Craig Lee	Aerospace Corp.
Standards, Goals, Gaps & Needs	Elysa Jones	CTO Secure Exchange Technology Innovation; OASIS Emergency Mgmt
Disaster Response	Christine Thompson	Co-Founder and President, Humanity Road
Public-Private Partnerships Enable Rapid Deployment of Security Capabilities	Dr. Tom Cellucci	CEO, Cellucci Associates; Past DHS Director of R&D and Chief Commercialization Officer
Secure Healthcare Network System in the Cloud	Bob Henley	CEO, Private Digital Network Services (PDNS)
Ground Rules for Working Session	Andy Born	Cybersecurity IPT Chair

Appendix B. Table of Barriers and Solutions (Correlated)

The top 5 barriers and security concerns that inhibit interoperability in federated cloud environments for information exchange and coordination in disaster response and health care are:

- Lack of clear RRAs (Roles, Responsibilities and Authorities)
- Lack of common standards & lexicon & terminology
- Inability to share status of critical infrastructure after disaster
- Concerns over data privacy & intellectual property rights
- Lack of coordination between government, corporations, volunteers, NGOs, churches, etc

Key: Type of barrier

- B = Business
- C = Cultural
- G = Governance
- T = Technical

#	Type	Barrier	Solution
Lack of Clear RRAs (Roles, Responsibilities, Authorities)	GC	Uncertainty over roles in disaster (who's in charge of what)	
	GC	Uncertainty over who's in charge of networks during disaster response	
	GC	Uncertainty over who's in charge of security during disaster response	
	C	Lack of agreements on legal definitions	
	C	Lack of guiding principals (persons)	
	C	Lack of guiding principles (ideas)	

Figure B1. Lack of Clear RRAs (Roles, Responsibilities and Authorities)

#	Type	Barrier	Solution
Lack of Common Stardards & Lexicon & Terminology	G	Different terminology & forms to be filled out when needed to shuttle patient from ground to hospital (especially across international lines)	
	C	Cultural differences creates diversity in terminology, understanding standards , practices, and acceptable actions. Overcoming the effects of cultural diversity is one of the largest problems	Create guidelines for how to respond Creat a lexicon on terminology Create the categories to be used for reporting
	C	How do you get cloud providers to play together without X (like penguins) No one wants to be first	You can have multiple standards, as long as you have interoperability among them
	GTC	Standards are not universally adopted and will always vary in implementation depth (e.g. PKI, SQL, etc.)	
	T	Need Standards that are approved (interoperable data standards), not standards of practice (guideliness)	
	T	There are no standards for mapping of reports on status of comms, transportation	Need to develop translators between existing systems, or develop standards for mapping of reports on status of comms, transportation
	T	There is no baseline of standard/critical needs on crowd maps	
	T	No standard set of terminologies	
	T	Network operators & users don't know standards and protocols to use after a disaster	Develop method for network operators to predict (before disaster) what standards and protocols to use in a particular type of disaster. So in disaster type A, use protocol X, in disaster type B, use protocol Y, etc.
	T	No standards of how to get reports – mapping , 42 crowd maps	
	B	No one is going to bet the farm until a standard is widely accepted. How facilitate growth of best practice so that it gets critical mass of widely used.	NCOIC
	T	Network operators & users don't know standards and protocols to use after a disaster	Develop method for network operators to predict (before disaster) what standards and protocols to use in a particular type of disaster. So in disaster type A, use protocol X, in disaster type B, use protocol Y, etc.
	T	Common lexicon of terms	
	GC	Everyone agreeing to use Common lexicon of terms. Need a governance template to standardize the guidelines to use.	

Figure B2. Lack of Common Standards, Lexicon & Terminology

#	Type	Barrier	Solution
Inability to Share Status of Infrastructure	GT	Lack of understanding of what's already working with first responders (what they're using, and whether it's operational/broken)	
	T	When aid workers show up after natural disaster, it's difficult to know what IT infrastructure (networks & communications) are still functioning – need to have a communications assessments (nothing to measure signals)	
	T	Need ability to broadcast availability of Haves (intact resources) after disaster: HAVE = there's a bed or room available at this location. These HAVEs can then be put onto map for disaster relief workers to find & use	
	T	If don't know data's there, then data is useless. Need ability for Data Awareness & Discoverabilty	
	T	Need to develop list of data feeds, and broadcast to air workers	
	T	Network operators & users don't know standards and protocols to use after a disaster	Develop method for network operators to predict (before disaster) what standards and protocols to use in a particular type of disaster. So in disaster type A, use protocol X, in disaster type B, use protocol Y, etc.
	T	Need to correlate call for help with location of closest working hospital (so need to find list of hospitals in area, and determine status & capabilities of each: military or civilian or newly created field hospital). Does it have helicopter landing area?	
	T	After a disaster, there are often multiple separate crowd maps showing availability & needs, which need to be integrated/fused	Use an initiative from the US DoS Humanitarian Information Unit (HIU). Imagery to the Crowd allows use of the US Government's commerical satellite imagery data license known as Next View, for creating derived works in OpenStreetMap, for humanitarian purpose
	T	Network operators & users don't know standards and protocols to use after a disaster	Dynamic re-planner templates used during Geo-spatial cloud event
	T	Sharing data - 42 crowd maps were created, but needed integration into 1 big unified map	Use solution like Gas Buddy - what gas station has gas (crowd source or Yelp)
	T	There is no baseline of standard/critical needs on crowd maps	
	T	Hard to determine which communications were down – could not measure signal availability. No one responsible for determining communications were down, and disseminating this info	
	GB	Lack of data awareness (where's the sources & distributors of data that are still working after disaster)	Point (not a solution): During a crisis – you can quickly see what works, so do what works
	GT	Cannot measure the signal levels to know how to communicate with	
	T	Need to develop list of data feeds, and broadcast to air workers	
	T	There are no standards for mapping of reports on status of comms, transportation	Need to develop translators between existing systems, or develop standards for mapping of reports on status of comms, transportation
	T	Open Street Map (OSM) required 4 technical enablers: Need release of imagery	Use Open Street Map's solution used in disaster response
	T	Open Street Map (OSM) required 4 technical enablers: Need imports of exisitng datasets	Use Open Street Map's solution used in disaster response
	T	Open Street Map (OSM) required 4 technical enablers: Need data schema with flexibile evolving models	Use Open Street Map's solution used in disaster response
	T	42 crowd maps were made by different people	
	T	Open Street Map (OSM) required 4 technical enablers: Need tollset with open-source stack	Use Open Street Map's solution used in disaster response

Figure B3. Inability to Share Status Of Critical Infrastructure After Disaster

#	Type	Barrier	Solution
Data Privacy & Intellectual Property Rights & Multi-Level Security	G	Concerns over sharing of PII & PHI (personally identifiable information & protected health information)	
	B	Concerns over protection of IP (intellectual property)	Establish CRADA with Govt and PIA/NDA with other companies
	T	One-size-fits-all privacy constraints don't work	Solution 1. Use varying privacy constraints (In disaster A, allow privacy constraint X. In disaster B, allow privacy constraint Y). Solution 2. Use set of templates that are tailorable, Use set of templates that are tailorable (So joint force task guys use X)
	GBC	During & after disaster, principals don't want videos from cameras to be shared	Solution 1. Data owner determines the rules for their data. Solution 2. Dynamic rules might permit data sharing under changing circumstances
	G	Governance compliance (HIPAA and the Data Protection	
	GT	Inability of orgs to exchange info during emergency, especially law enforcement info	Establish and utility NIEM (national info exchange model) for exchanging law enforcement info
	B	Intellectual property issues	

Figure B4. Concerns over Data Privacy & Intellectual Property Rights

#	Type	Barrier	Solution
Lack of Coordination	C	Lack of coordination between "helpers"	
	T	No standard set of terminologies	
	BT	No common set of best practices	
	BT	Interoperability principles for disaster	
	C	Difficult to get groups to work together (government, churches, un-affiliated volunteers, NGOs, corporations)	

Figure B5. Lack of Coordination between Government, Corporations, Volunteers, NGOs, Churches, Etc