Global Information Assurance Certification Paper

"Security within the Public Health Information Network (PHIN)"

GSEC Practical v.1.4 Option 1

Joseph L. Nay
April 14, 2004

Table of Contents:

Abstract

Today's world is dependant of the ability of the public health professionals to protect our county. The responsiveness of public health officials can no longer be at a paper based speed; with the threat of bio-terrorism, SARS, Anthrax, West Nile Virus, and even influenza shortages the need for public health initiatives to move to a secure, streamline electronic based system is greater now than it has ever been. Projects such as Health Alert Network (HAN), National Electronic Disease Surveillance System (NEDSS), Laboratory Response Network (LRN), Epidemiology Information Exchange (EPI-X), and National Health Care Safety Network (NHSN) have shown that the use of information technology can further the cause of public health, but have also revealed the need for a secure network to exchange data to outside sources. The Public Health Information Network (PHIN) is a vision of enabling health organizations to perform the required functions with the use of current information technology systems when the functions cross program or organizational boundaries. These functions can include real-time data processing, computer assisted analysis, decision support, professional collaboration, and rapid dissemination of information to public health, clinical care and the general public.[1]

PHIN consists of a set of standards in development at the department of Health and Human Services (HHS) through the Center for Disease Control and Prevention's (CDC). PHIN has set up standards for Electronic Data Interchange (EDI), the exchange of data from one repository or system to another. In the healthcare field EDI for clinical and administrative data is done through a data format standard known as Health Level Seven (HL7.) HL7 is widely accepted and is an American National Standards Institute (ANSI) approved standard for clinical healthcare EDI communications.[2] The use of the HL7 standard has been recommended for all Federal agencies who exchange healthcare information.[3] PHIN has also standardized the messaging protocol to the use of ebXML called PHIN Messaging System (PHIN MS).[4] This paper will discuss the difference security aspects of the PHIN architecture.

[1] Loonsk, John W. Public Health Information Network, May 13, 2003 URL http://www.cdc.gov/phin/conference_presentations/05-13-03/opening/2003%20PHIN%20Conference%20Opening%20Plenary%20-%20John%20Loonsk.pdf, April 14, 2004

[2] What is HL7? Messaging Standard Version 2.5, June 26, 2003 URL http://www.hl7.org/about, March 16, 2004

[3] Standards at Center Stage, ***Healthcare Informatics,*** November 2003 URL http://www.healthcare-informatics.com/issues/2003/11_03/ball.htm April 12, 2004

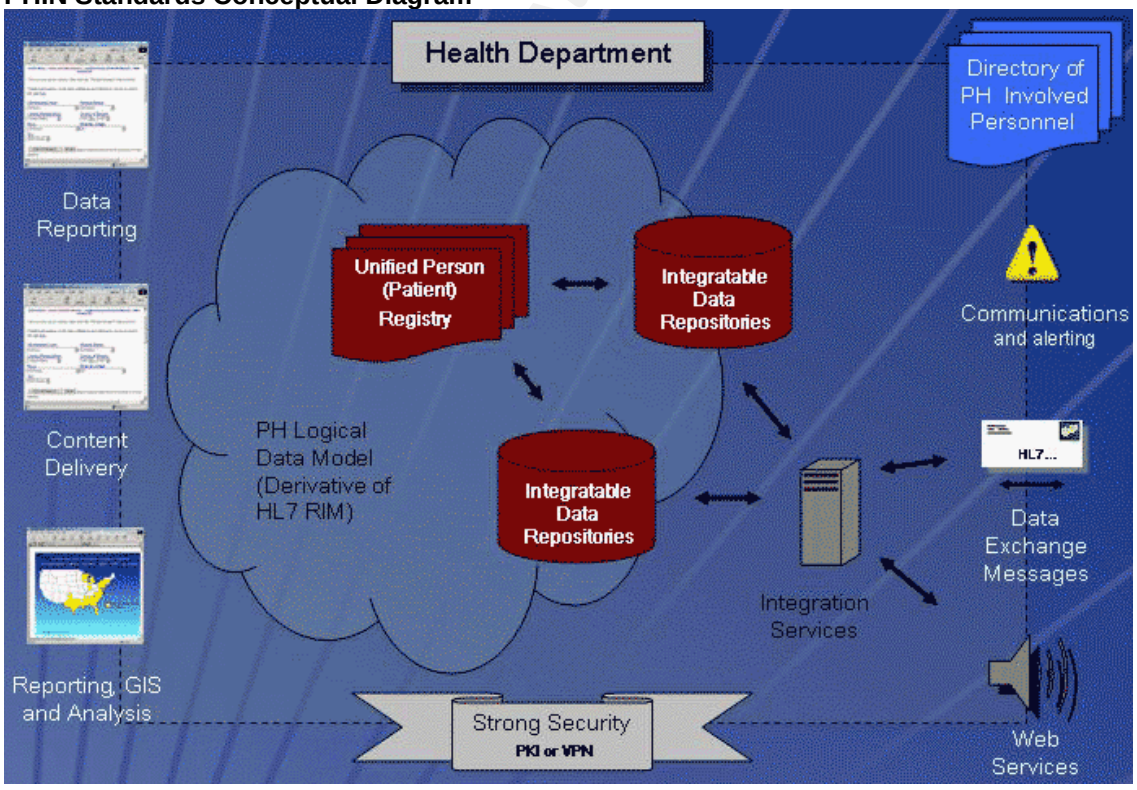
[4] Public Health Information Network Functions and Specifications Version 1.2 – December 18, 2002 URL http://www.cdc.gov/phin/Public%20Health%20Information%20Network%20Functions%20and%20Specificat%85.pdf, March 15, 2004

Overview

The concept of PHIN began from the National Electronic Disease Surveillance System. (NEDSS) NEDSS was one of the first efforts to develop a public health infrastructure for the exchange of necessary information between local, state, and federal health officials. NEDSS was developed for the collection of case data for the purpose of disease surveillance and tracking and for the required reporting of this data to authorized health officials. This process had previously been preformed either through paper reports or independent legacy systems. NEDSS was the leader in breaking down the boundaries between programs and streamlining the process.

In August 2002 the CDC Information Council (CIC) approved the creation of the PHIN program. This system would have the ability to cross lines of local, state, and federal programs to facilitate the sharing of necessary information to further the cause of public health. NEDSS has been one of the cornerstones of the PHIN model; it has shown the extreme need for these systems. The CIC consisted of representatives from CDC internal departments that were stakeholders of the PHIN system. A conceptual model for the PHIN standards was developed and the CIC began working toward making PHIN a reality.

PHIN Standards Conceptual Diagram[5]



[5] PHIN Standards Conceptual Diagram, URL http://www.cdc.gov/phin/about/standards.htm, April 15, 2004

Data that will be included in the PHIN system will include patient identifiable information, bio-terrorism, disease outbreaks, vaccination rates, laboratory data, patient safety data, and more. Because this is information is protected information, data security is a high priority in the PHIN model. The functional specifications for PHIN security states the objective of PHIN security as "To ensure that sensitive or critical electronic information and systems are not lost, destroyed, misappropriated or corrupted."[6]

HIPAA and other legislative rules have exemptions for disclosures for public health activities and purposes when that disclosure is to a public health authority, foreign government acting with a public health authority, or a person exposed or at risk of contracting or spreading a disease.[7] So these regulations have minimal impact in the PHIN system.

PHIN has five key areas detection and monitoring, data analysis, knowledge management, alerting, and response. Each of these areas can stretch across many different programs and have the need to share information. PHIN must be flexible enough to cover these elements, have strict enough standards to allow communication between systems, and have enough security to provide a comfort to the owners of systems to implement the sharing of required data.

The components of the PHIN architecture that have been researched to this paper are the use of standards, Health Level Seven (HL7), the Secure Data Network (SDN), and the Public Health Information Network Messaging System (PHIN MS). While this is not a comprehensive listing of the components of the PHIN system, each of these elements have roles to play in the security CIA Triad, Confidentiality, Integrity, and Availability.[8] This paper will review each component and detail the specific role it plays in the overall security of the PHIN system.

The concept of PHIN is long overdue and will be of a great benefit to the country's health and wellbeing as long as it is developed with the focus on the programmatic features and functionalities needed. PHIN is not exclusively a HHS/CDC job, grant money has been set aside for local and state governments to participate in PHIN.[9] The importance of security when designing and implementing a project of this magnitude can not be understated.

---

[6] IT Security and Critical Infrastructure Protection, December 23, 2003, URL http://www.cdc.gov/cic/functions-specs/function_9.htm, April 15, 2004

[7] Standards for Privacy of Individually Identifiable Health Information: Implications for Public Health Practice, March 2000, URL http://www.cdc.gov/cic/documents/publichealthprivacy.ppt, April 15, 2004

[8] Chapple, Mike. The GSEC Prep Guide. Indianapolis, IN, Wiley Publishing, Inc. 2003. 2-3

[9] Dizard, Wilson P., "How major IT projects made out, by agency " Government Computer News/GNC.com, February 9, 2004, URL http://www.gcn.com/23_3/news/24873-1.html, April 15, 2004

Standards

The importance of standards has been well documented through the years, as the saying goes "The great thing about standards is that there are so many to choose from." This puts the pressure on the PHIN system to choose the appropriate applicable standards and facilitate the widespread use of these. Unless these standards are adopted and utilized, PHIN will be unable to become the foundation for communication in the public health world.

Public Health information systems have historically been developed in silos, independent systems that would fill the specific need of that particular health program. There was no thought to sharing the information between programs or anywhere other than that which was minimally required. Programs did not give close attention to the method of development and rarely used approved standards. If standards were used they were chosen within the silo of the project. This paradigm of working alone will need to be shifted to a process of cooperation and sharing.

On March 21, 2003 Tommy Thompson, secretary of HHS, announced that "the first set of uniform standards for the electronic exchange of clinical health information to be adopted across the federal government." He stated the important role the Federal Government plays in being the leader in the use of standards and the importance of security in the use of these standards. [10]

In this press release Secretary Thompson listed several standards that would be included in this including HL7, laboratory Logical Observation Identifier Name Codes (LOINC), and National Council on Prescription Drug Programs (NCDCP). [10]

The need and importance of PHIN is evident, now the work of developing a system that will fit the needs of all public health information systems across local, state, and federal governments is the challenge faced by the CIC. Ensuring that system is secure is one of the high priorities for the CIC. If the challenge set by Secretary Thompson is to be met, that the government will be the leader in the development and use of standards, then making sure the use of these standards are implemented across the PHIN and every implementation is secure, will be paramount for the CDC.

Standards role in the CIA triad for the security of the PHIN system is ensuring the availability of the information. If the standards of communication, vocabulary, or data fields are neglected the information will not be able to be transmitted and if by some stroke of luck the information arrives at it intended destination the ability for the receiving system to interpret the information will be an insurmountable

[10] Thompson, Tommy, FIRST FEDERAL eGOV HEALTH INFORMATION EXCHANGE STANDARDS, March 21, 2003, URL http://www.hhs.gov/news/press/2003pres/20030321a.html, April 15, 2004

task, the integrity of the data will be lost. Promoting the use of standards throughout the PHIN is the only way to ensure the information gets to its target protected from harm and that the data is in its expected format.

Health Level Seven (HL7)

Health Level Seven (HL7) is an American National Standards Institute (ANSI) approved standard. It is a set of message structures that makeup the core information that is needed for administrative and clinical healthcare institutions.

HL7 was the natural choice for the messaging standard because it is ANSI approved and mandated by Secretary Thompson for all Federal Agencies to use when communicating healthcare information. HL7 is not only the standard chosen by the Federal Government, but it is the leading standard in the private healthcare industry.

The mission of HL7 is "To provide standards for the exchange, management and integration of data that support clinical patient care and the management, delivery and evaluation of healthcare services. Specifically, to create flexible, cost effective approaches, standards, guidelines, methodologies, and related services for interoperability between healthcare information systems."[11] This sounds very similar to the work that PHIN is conducting.

It is no surprise that HL7 and PHIN have similar missions because HL7 was created to support implementations of sharing healthcare information across systems. There are numerous HL7 engine software packages available and all are compatible with each other, this is one of the great advantages of using standards.

An HL7 Implementation Guide needs to be authored for each message type use in the PHIN. These guides are vital to the integrity of the data because HL7 is a very “loose” standard. Because it makes provisions for implementations worldwide the standard is left very open to data interpretation, two data fields within the standard may be interpreted to mean the same data element, causing a loss of data when transferring data from one system to another. The use of an implementation guide will greatly reduce the occurrence of these types of data integrity issues.

HL7 is the messaging structure, the format which the data will be in when it is sent from one system to another and a data vocabulary. The security that is built into HL7 in minimal, it has locations for the receiving system to identify the sender and to have a qualified notation from that sender to identify them. But this method of securing HL7 is easily spoofed and does not meet the requirements of PHIN, thus the security for PHIN is based in other standards.

[11] What is HL7?, URL http://www.hl7.org/, April 15, 2004

Even though the direct role of HL7 in security is limited, HL7 does have a very important role in the integrity of the information that is being shared. Without the specifications contained in HL7 receiving system would have no idea of what the information means. Implementations would need to support numerous proprietary data standards and significant effort would be need between every implementation.

Secure Data Network (SDN)

The SDN is the standard implemented at CDC for transmitting data from outside the firewall. This is accomplished through an encryption server, application server and x.509 digital certificates for verification. This allows a secure method for the client applications to transmit data securely inside the firewall at CDC. The standard for communicating the digital certificates is hypertext transport protocol (HTTP) with secure socket layer encryption (SSL) or HTTPS. This is a standard internet protocol build within standard browsers so difficulties with firewalls and other security measures implemented in individual projects would not interfere with the implementation of the PHIN.

The current certificate authority (CA) for the digital certificates issued is VeriSign Inc. one of the industry leaders in digital certificates. The maintenance of the certificates will be governed by a business steward at CDC for each program that the individual will be submitting data to; this individual would ensure proper identification for each user issued a certificate and that proper security training for proper use of the certificate. SDN can support several activities for each certificate, so users who work in several system that communicate through PHIN to CDC only require one certificate issued to them, after the initial certificate they just need to request access to the required program or activity associated with the program. The servers are maintained by the Information Resource Management Office (IRMO). The digital certificates issued each have a maximum life of one year, requiring each user to renew their certificate at least an annual basis.

The SDN is now the only standard to be use to communicate to CDC from outside the firewall. "The SDN standards and procedures govern all Internet-based secure access to CDC/ATSDR. The SDN shall be the Internet security system used by all CDC/ATSDR programs unless an explicit exemption has been granted."12

Where HL7 had only limited security functionality and dealt only with the integrity of the data itself, SDN is solely concerned with the confidentiality and availability of the system. There are several layers of security within the SDN including the SSL encryption, X.509 digital certificate encryption, and a pass phrase authorization to access the SDN server.

This level of security allows the users of the PHIN to have a high level of confidence in the integrity of the information sent to CDC or received from CDC.

[12] Secure Data Network Overview, July 7, 2001, URL http://www.cdc.gov/irmo/ea/sdn.htm, April 15, 2004

SDN it the gateway into the PHIN systems, the availability of the SDN servers will determine how effective and secure the communications between systems with PHIN implementations will be.

PHIN Message System (PHIN MS)

The PHIN MS (a specific implementation of ebXML-MS) is only concerned with the actual transporting of the information from one system to another in a secure and efficient manner. The contents of that message are the responsibility of the application that creates the data and the HL7 messaging standard.[13]

ebXML was recently approved by the International Organization for Standardization (ISO) as a EDI communications tools.[14]

Within the PHIN MS design there are three elements message sender, a message receiver, and a message handler. The message sender listens to the database application for a trigger event (this is typically a record being written to a specific table structure in the database or an HL7 engine placing a HL7 message into a message queue) then captures the record, encrypts it based on the user identification, places it in an ebXML wrapper, encrypts it with the X.509 digital certificate and sends it through the SDN process which transmits it over the internet via https to the message receiver. The PHIN MS message receiver takes the message decrypts and processes it through the receiving client. The PHIN MS sending client also retrieves the challenge phrase for the certificate server that process the message between the PHIN MS servers.[15]

The PHIN MS encryption can use both digital certificates and public key encryption. It is flexible enough to conform to HIPAA security regulations. The implementation of ebXML is not unique; it is an accepted standard for business to business communications.

PHIN MS is written in Java to promote the flexibility of the service. This allows for portability across platforms. It also allows for integration into most any type of development environment. This plays to the strengths of the specific implementations of PHIN. No one project can dictate the development platform needed to use PHIN.

The PHIN MS plays a vital role in the security of the entire PHIN system. This incorporated with the SDN provides a multi-layered security architecture with

---

[13] ebXML Messaging, 2004, URL http://www.drummondgroup.com/html-v2/ebxml.html, April 14, 2004

[14] ebXML: Suite of specifications promises to cut costs and simplify processes for e-business, March 26, 2004 URL http://www.iso.org/iso/en/commcentre/pressreleases/2004/Ref904.html, April 16, 2004

[15] Public Health Information Network Messaging System (PHIN MS), Sept. 5, 2003 URL http://www.cdc.gov/phin/components/PHIN%20Brochure%20PHIN%20MS%20.ppt, April 14, 2004.

multiple encryptions. This design will meet the regulatory statutes necessary and allow for specific implementations to add their own infrastructure security without interference to PHIN.

It is an essential that PHIN be open enough to integrate with the security infrastructure across any platforms and have the ability to communicate in batch or real-time. This flexibility will allow system to have the availability to the data when they need it.

As outline above, PHIN MS deals with the availability and confidentiality of the PHIN system. Its key role in the security lies in the transporting of the messages in a secure and efficient manner, thus maintaining these aspects of the triad.

Summary

The need for the creation of the Public Health Information Network is without question an incredible leap forward for the public health field. To put current information technology advances to use for the health benefits of our country and world is long over due. But care should be taken whenever data as sensitive as health data is involved.

The development of the standards comprise in the PHIN system were chosen due to the acceptance in the standards community. Each one has been reviewed by the CDC Information Council (CIC) and compared to other related standards. These standards showed that they would provide the PHIN with the needed elements to successfully be implemented in any required system.

The benefit of having ISO and ANSI approved standards is they have been tried and tested by a wide range of people. They have been implemented in many different environments and been secured.

Securing the PHIN will require cooperation from the projects implementing it, ensuring that all three areas of the security triad are successfully covered during the implementation. The confidentiality of the information will also require authentication on the part of the specific software system that generates the data in addition to the authorization for the SDN site and the PHIN MS. The availability of the system will depend on both the sending and receiving software applications. Even if the PHIN MS and SDN tools are accessible 24/7, if the particular software application is off the message will just sit in a queue until it becomes available. HL7 can be defined to the exact specification of each data element, but if the sending application sends garbage in……you get garbage out.

The CIC has done an excellent job of providing specifications to develop a PHIN system that will be secure and they have recommended tools and standards that will make the development of the system a straight forward process. Secretary Tommy Thompson's vision of the Federal government being the leader in setting

the standards for healthcare electronic communications is well on it's way. EDI is not a simple process, but PHIN has laid out the plans for a "consistent exchange of response, health, and disease tracking data between public health partners." [16]

I will close with a statement about the importance of security for the PHIN system "Ensuring the security of this information is also critical, as is the ability of the network to work reliably in times of national crisis."[16] The PHIN system is architected in such a way as to provide enough security achieve the goals of public health.

[16] Overview of PHIN, April 8, 2004 URL http://www.cdc.gov/phin/, April 16, 2004

References

Loonsk, John W. Public Health Information Network, May 13, 2003 URL http://www.cdc.gov/phin/conference_presentations/05-13-03/opening/2003%20PHIN%20Conference%20Opening%20Plenary%20-%20John%20Loonsk.pdf, April 14, 2004

What is HL7? Messaging Standard Version 2.5, June 26, 2003 URL http://www.hl7.org/about, March 16, 2004

Standards at Center Stage, *Healthcare Informatics,* November 2003 URL http://www.healthcare-informatics.com/issues/2003/11_03/ball.htm April 12, 2004

Public Health Information Network Functions and Specifications Version 1.2 – December 18, 2002 URL http://www.cdc.gov/phin/Public%20Health%20Information%20Network%20Functions%20and%20Specificat%85.pdf, March 15, 2004

PHIN Standards Conceptual Diagram, URL http://www.cdc.gov/phin/about/standards.htm, April 15, 2004

IT Security and Critical Infrastructure Protection, December 23, 2003, URL http://www.cdc.gov/cic/functions-specs/function_9.htm, April 15, 2004

Standards for Privacy of Individually Identifiable Health Information: Implications for Public Health Practice, March 2000, URL http://www.cdc.gov/cic/documents/publichealthprivacy.ppt, April 15, 2004

Chapple, Mike. The GSEC Prep Guide. Indianapolis, IN, Wiley Publishing, Inc. 2003. 2-3

Dizard, Wilson P., "How major IT projects made out, by agency " Government Computer News/GNC.com, February 9, 2004, URL http://www.gcn.com/23_3/news/24873-1.html, April 15, 2004

Thompson, Tommy, FIRST FEDERAL eGOV HEALTH INFORMATION EXCHANGE STANDARDS, March 21, 2003, URL http://www.hhs.gov/news/press/2003pres/20030321a.html, April 15, 2004

What is HL7?, URL http://www.hl7.org/ , April 15, 2004

Secure Data Network Overview, July 7, 2001, URL http://www.cdc.gov/irmo/ea/sdn.htm, April 15, 2004

ebXML Messaging, 2004, URL http://www.drummondgroup.com/html-v2/ebxml.html, April 14, 2004

ebXML: Suite of specifications promises to cut costs and simplify processes for e-business, March 26, 2004 URL http://www.iso.org/iso/en/commcentre/pressreleases/2004/Ref904.html, April 16, 2004

Public Health Information Network Messaging System (PHIN MS), Sept. 5, 2003 URL http://www.cdc.gov/phin/components/PHIN%20Brochure%20PHIN%20MS%20.ppt, April 14, 2004.

Overview of PHIN, April 8, 2004 URL http://www.cdc.gov/phin/, April 16, 2004

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event