FDA’s CENTER FOR DEVICES & RADIOLOGICAL HEALTH, THE DEPARTMENT OF HOMELAND SECURITY (DHS) C³ VOLUNTARY PROGRAM AND THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM PRESENT A PUBLIC WORKSHOP:

Collaborative Approaches for Medical Device and Healthcare Cybersecurity

October 21-22, 2014
National Intellectual Property Rights Coordination Center
Arlington, VA
Dear Colleagues,


Our objective is to catalyze collaboration among all stakeholders within the healthcare and public health (HPH) community in order to address current cybersecurity gaps and challenges, as well as to be forward thinking, anticipating and preparing for how we can strengthen our nation’s healthcare and public health critical infrastructure cybersecurity beyond today.

We envision this workshop as an important step towards our HPH community’s collective understanding of the National Institute of Standards and Technology (NIST) “Framework for Improving Critical Infrastructure Cybersecurity” published in February 2014, and how it might be adapted to address the unique medical device cybersecurity needs and challenges within healthcare and public health.

Advancing cybersecurity measures within healthcare and public health relies upon a ‘whole of community’ approach, and that requires us all to accept shared ownership and shared responsibility. By convening this public meeting, we aim to foster collaboration such that emerging threat and vulnerability information is readily shared; and in partnership with you, we seek solutions that incentivize organizations to adopt best practices and industry standards that can be included in product design and systems architecture.

We express overwhelming appreciation to all of you who have made this public meeting possible. Much gratitude goes to our workshop partners – DHS and HHS – and FDA’s Center for Devices and Radiological Health (CDRH) Cybersecurity Working Group, the Emergency Preparedness/Operations & Medical Countermeasures (EMCM) Program, the Office of Communications and Education staff, and the Digital Communication Media Staff for your tireless and herculean efforts in planning, organizing and executing this meeting. Special acknowledgement goes to all of our expert speakers, moderators and panelists who have prepared diligently - some traveling great distances to join with us and share their critical insights, experiences and perspectives. We value your contributions to this important dialogue and see this as merely a first step towards future collaborative efforts.

Last, but far from least, we want to take this opportunity to thank all of you for your enthusiasm, passion and commitment to work together with us in building a comprehensive cybersecurity infrastructure that can detect and respond to threats and vulnerabilities in a timely way and that strives to achieve cyber resiliency for safeguarding our nation’s public health.

Sincerely,

Suzanne B. Schwartz, MD, MBA
FDA Disclaimer

The views expressed in this Public Workshop are those of the authors and do not necessarily reflect the official policy or position of the U.S. Food and Drug Administration, the Department of Health and Human Services, or the United States Government, and should not be used for advertising or product endorsement purposes. Reference to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its approval, endorsement, recommendation, or favoring by the United States Government or any department, agency, office, or branch thereof.
Contents
Collaborative Approaches for Medical Device and Healthcare Cybersecurity ........................................... 1

WELCOME .................................................................................................................................................. 3

FDA Disclaimer ........................................................................................................................................... 4

Contents ..................................................................................................................................................... 5

Agenda at a Glance .................................................................................................................................... 9

    Agenda Day 1: October 21, 2014 ........................................................................................................... 9

    Agenda Day 2: October 22, 2014 ......................................................................................................... 15

Cybersecurity Public Workshop Session Descriptions, Objectives, and Questions for Consideration ...... 19

Speaker Biographies ................................................................................................................................. 35

Steven Abrahamson, MBA Director of Product Security Engineering GE Healthcare ......................... 35

Bill Aerts, CISSP, CISM Director of Information and Product Security Medtronic’s Global Privacy and Security Office ............................................................................................................................ 36

Mike Ahmadi, CISSP Global Director of Medical Security Codenomicom ............................................ 37

Debra Bruemmer, MBA, CISSP Principle Information Security Analyst Mayo Clinic in Rochester, Minnesota .................................................................................................................................................. 38

Helen Caton-Peters MSN, RN Health IT Privacy and Security Specialist Office of the Chief Privacy Officer Office of the National Coordinator ................................................................................................................. 39

Penny Chase, MS, MA The MITRE Corporation ......................................................................................... 40

Steve Christey Coley Principal Information Security Engineer Cyber Security Division The MITRE Corporation ................................................................................................................................................................. 41

Bryan Cline, PhD, CISSP-ISSEP, CISM, CISA, ASEP, CCSFP, HCISPP Senior Advisor to the Health Information Trust Alliance (HITRUST) ........................................................................................................... 42

Rick Comeau, MBA Strategic Advisor to the Center for Internet Security’s (CIS) CEO & President Center for Internet Security ................................................................................................................................. 43

Stephen Curren, MS Acting Director of the Division of Resilience and Infrastructure Coordination Within this Division is the Critical Infrastructure Protection Program Office of Assistant Secretary for Preparedness and Response U.S. Department of Health and Human Services (HHS) ......................................................................................................................... 44

Michael Daniel, MS, MPP Special Assistant to the President and Cybersecurity Coordinator .......... 45
Sherman Eagles Partner SoftwareCPR

Marty Edwards Assistant Deputy Director, National Cybersecurity and Communications Integration Center (NCCIC) Director, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Department of Homeland Security..................................................................................................................47

Joshua “Josh” Emperado, MSBME, MSEE Sr Manager, Market Development MR Toshiba America Medical Systems ........................................................................................................................................48

Thaddeus Flood, JD Industry Director for X-Ray and Medical Imaging Informatics MITA.................49

Michael Frederick, MS Vice President of Assurance Services and Product Development HITRUST .50

Kevin Fu, PhD Associate Professor of Electrical Engineering and Computer Science Director for the Archimedes Center for Medical Device Security University of Michigan ..........................................................................................51

Edward J. Gabriel, MPA, EMT-P, CEM, CBCP Principal Deputy Assistant Secretary for Preparedness and Response Department of Health and Human Services........................................................................52

Elisabeth M. George, MS Vice President of Global Regulation & Standards Philips Healthcare........53

Julian M. Goldman, MD Medical Director of Biomedical Engineering Partners HealthCare Practicing anesthesiologist at the Massachusetts General Hospital ..........................................................................................54

Jeffery M. Goldthorp Associate Bureau Chief – Cybersecurity and Communications Reliability Public Safety and Homeland Security Bureau Federal Communications Commission ........................................55

Rick Hampton Wireless Communications Manager Partners Healthcare System, Boston, MA......56

Kevin Hemsley, CISSP Project Manager Idaho National Laboratory Supporting the US Department of Homeland Security Industrial Control Systems Cyber Emergency Team (ICS-CERT)..........................57

Ken Hoyme, MS Distinguished Scientist Adventium Labs...................................................................58

Lee Kim, JD, FHIMSS Director of Privacy and Security Healthcare Information and Management Systems Society (HIMSS)................................................................................................................59

Deborah Kobza, CGEIT, JIEM Executive Director/CEO National Health Information Sharing & Analysis Center (NH-ISAC) Security Intelligence, Information Sharing & Response........................................60

Ramya Krishnan, MS Senior Project Engineer Health Devices Group ECRI Institute..........................61

Darren Lacey, JD Chief Information Security Officer and Director of IT Compliance Johns Hopkins University and Johns Hopkins Medicine ................................................................................................................62

Mary K. Logan, JD, CAE President and CEO of the Association for the Advancement of Medical Instrumentation (AAMI)........................................................................................................................................63
John Lu, MBA, MS, CISSP Principal Deloitte & Touche LLP ................................................................. 64
William H. Maisel, MD, MPH Chief Scientist and Deputy Center Director for Science FDA Center for Devices and Radiological Health ................................................................. 65
Jackie McCarthy, JD Director of Wireless Internet Development at CTIA-The Wireless Association® ................................................................. 66
Kevin McDonald, BSN, ME-PD, CISSP Director of Clinical Information Security Mayo Clinic ............ 67
Michael C. McNeil, MBA Global Product Security & Services Officer Philips Healthcare .................. 68
Ron Mehring, MBA, CISSP Senior Director - Information Security & CISO Texas Health Resources .... 69
John F. Murray Jr., MS Expert Regulatory Review Scientist Office of Compliance Center for Devices and Radiological Health United States Food and Drug Administration ........................................... 70
Dale Nordenberg, MD Executive Director, MDISS CEO, Novasano Health and Science ..................... 71
Gavin O’Brien, MS Computer Scientist National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) ................................................................. 72
Thad Odderstol, MS Industry Engagement and Resilience Stakeholder Engagement and Cyber Infrastructure Resilience Cybersecurity and Communications U.S. Department of Homeland Security .................................................................................................................. 73
Bakul Patel, MS, MBA Associate Director for Digital Health (acting) Center for Devices and Radiological Health (CDRH) U.S. Food and Drug Administration (FDA) ................................................................. 74
Henri “Rik” Primo, MS Director of Strategic Relationships for the SYNGO (Imaging Informatics) Division Siemens Medical Solutions USA, Inc. .................................................................................................................. 75
Jay Radcliffe, MS, CISSP Senior Security Consultant and Researcher Rapid7 .................................... 76
Linda Ricci Branch Chief, Cardiac Diagnostic Devices Branch Division of Cardiovascular Devices Office of Device Evaluation Center for Devices and Radiological Health ................................................................. 77
Tim Skutt Director, Security Portfolio Wind River .................................................................................. 81
Wesley Snell Jr., CISSP Director of the Computer Security Incident Response Center (CSIRC) U.S. Department of Health and Human Services (HHS) ................................................................. 82

Kevin Stine Manager of the Security Outreach and Integration Group NIST’s Computer Security Division .............................................................................................................................................. 83

Raymond P. Strucker Senior Special Agent /Operations Manager Office of Criminal Investigations (FDA/OCI) U.S. Food & Drug Administration’s ........................................................................................................ 84

Commander Nikhil Thakur Engineer Officer in the United States Public Health Service Regulatory Policy Advisor for the Emergency Preparedness, Operations and Medical Countermeasures (EMCM) Program Office of the Center Director Center for Devices and Radiological Health (CDRH) ............... 85

Gregory J. Touhill, CISSP Deputy Assistant Secretary for Cybersecurity Operations and Programs Office of Cybersecurity and Communications Department of Homeland Security .................. 86

Axel Wirth, MSc, CPHIMS, CISSP, HCISPP National Healthcare Solutions Architect Symantec Corporation ........................................................................................................................................ 87

Chantal Worzala, PhD Director of Policy American Hospital Association ............................................. 88

Margie Zuk, MS Senior Principal Cyber Security Engineer The MITRE Corporation .......................... 89

[Federal Register Volume 79, Number 184 (Tuesday, September 23, 2014)] ................................................................. 91

Notes Section: ......................................................................................................................................................... 100
# Agenda at a Glance

## Agenda Day 1: October 21, 2014

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30am-9:00am</td>
<td>Registration</td>
<td>Suzanne Schwartz, MD, MBA – Director Emergency Preparedness/Operations and Medical Countermeasures Program (EMCM), Center for Devices and Radiological Health (CDRH) / U.S Food and Drug Administration (FDA)</td>
</tr>
<tr>
<td>9:00am-9:15am</td>
<td>Welcome &amp; Introductory Remarks</td>
<td>Suzuane Schwartz, MD, MBA – Director Emergency Preparedness/Operations and Medical Countermeasures Program (EMCM), Center for Devices and Radiological Health (CDRH) / U.S Food and Drug Administration (FDA)</td>
</tr>
<tr>
<td>9:15am-9:30am</td>
<td>Keynote Speaker</td>
<td>Brigadier General Gregory Touhill (Invited) Deputy Assistant Secretary for Cybersecurity Operations and Programs, Acting Director of National Cybersecurity and Communications Integration Center (NCCIC), Department of Homeland Security (DHS)</td>
</tr>
</tbody>
</table>
| 9:30am-11:00am  | Envisioning Collaboration for Medical Device and Healthcare Cybersecurity | Panel Moderator: William H. Maisel, MD, MPH Chief Scientist and Deputy Center Director for Science CDRH/FDA  
Discussants:  
- Helen Caton-Peters, MSN, RN – Health IT Privacy and Security Specialist, Office of the National Coordinator for Health Information Technology (ONC) / Department of Health and Human Services (HHS)  
- Stephen Curren, MS – Acting Director of the Division of Resilience and Infrastructure Coordination, Office of Emergency Management (OEM) / Assistant Secretary for Preparedness and Response (ASPR) / HHS  
- Rick Hampton – Wireless Communications Manager, Partners Healthcare System  
- Lee Kim, JD, FHIMSS – Director of Privacy and Security,
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00am-11:15am</td>
<td>BREAK</td>
<td></td>
</tr>
<tr>
<td>11:15am-11:25am</td>
<td>Keynote Speaker</td>
<td>Edward Gabriel, MPA, EMT-P, CEM, CBCP&lt;br&gt;Principal Deputy, Assistant Secretary of Preparedness and Response (ASPR)</td>
</tr>
<tr>
<td>11:25am-12:30pm</td>
<td>Cyberthreat Landscape – ‘Framing the Problem’</td>
<td><strong>Panel Moderator:</strong>&lt;br&gt;Stephen Curren, MS&lt;br&gt;Acting Director&lt;br&gt;Division of Resilience and Infrastructure Coordination(OEM) / ASPR / HHS&lt;br&gt;&lt;br&gt;<strong>Presenters:</strong>&lt;br&gt;- Marty Edwards – Assistant Deputy Director, NCCIC and</td>
</tr>
<tr>
<td>12:30pm-1:40pm</td>
<td>LUNCH</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>-------</td>
<td></td>
</tr>
</tbody>
</table>
| 1:40pm-2:30pm  | Aerospace Gaps and Challenges: Part I. Need to Share vs. Need to Secure | Panel Moderator:  
|                | Julian Goldman, MD  
|                | Medical Director of Biomedical Engineering  
|                | Partners Healthcare System;  
|                | Director, Medical Device Interoperability Program, Mass Gen Hospital  
|                | Discussants:  
|                | Sherman Eagles – Partner,  
|                | Director Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) / DHS  
|                | Jason Lay – Manager, Cyber Threat Information / Department of Health and Human Services (HHS)  
|                | Ray Strucker – Special Agent, Senior Operations Manager, Office of Criminal Investigation (OCI) / FDA  
|                | Discussants:  
|                | Terry Dunlap, MS – Partner and Managing Member, Tactical Network Solutions  
|                | Elisabeth George, MS – VP of Global Regulations & Standards, Philips Healthcare  
|                | Kevin Hemsley, CISSP – Project Manager, Idaho National Lab (INL) supporting ICS-CERT  
|                | Kevin McDonald, BSN, ME-PD, CISSP – Mayo Clinic  
|                | Billy Rios, MS, MBA, CISSP – Director of Vulnerability Research and Threat Intelligence, Qualys  
|                | Wesley Snell, CISSP – Director, Computer Security Incident Response Center (CSIRC) / HHS  
|                | CDR Nikhil Thakur – Regulatory Policy Advisor, EMCM / CDRH / FDA  
<p>|                | Axel Wirth, MSc, CPHIMS, CISSP, HCISPP – Distinguished Systems Engineer, Solutions Architect, Symantec |</p>
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Panel Moderator:</th>
<th>Discussants:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:30pm-3:15pm</td>
<td>Cybersecurity Gaps and Challenges: Part II. Legacy Devices</td>
<td>Kevin Fu, PhD</td>
<td>Steven Abrahamson, MBA – Director, Product Security Engineering, GE Healthcare</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Penny Chase, MS, MA – Information Technology and Cyber Security Integrator in the Information Technology Technical Center, MITRE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Josh Emperado, MS – Senior Market Development Manager, Toshiba America Medical Systems, &amp; Vice Chair Medical Imaging Informatics Section, Medical Imaging and Technology Alliance (MITA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Brian Fitzgerald – Deputy Director of the Division of Electrical and Software Engineering, Office of Science</td>
</tr>
<tr>
<td>3:15pm-3:30pm</td>
<td>BREAK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:30pm-4:15pm</td>
<td><strong>Cybersecurity Gaps and Challenges: Part III. Forward Looking Design</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Panel Moderator:</strong> Thaddeus Flood, JD Industry Director for X-Ray and Medical Imaging Informatics Medical Imaging and Technology Alliance (MITA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Discussants:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bill Aerts, CISSP, CISM – Director of Information &amp; Product Security, Global Privacy and Security Office, Medtronic</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Debra Bruemmer, MBA, CISSP – Principle Information Security Analyst, Mayo Clinic</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Abiy Desta – Senior Policy Analyst / ODE / CDRH / FDA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ken Hoyme, MS – Distinguished Scientist, Adventium Labs and Co-chair Device Security Workgroup Association for the Advancement of Medical Instrumentation (AAMI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Darren Lacey, JD – Johns Hopkins University/Johns Hopkins Medicine</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Michael McNeil, MBA – Global Product Security and Services Officer, Philips Healthcare</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Billy Rios, MS, MBA, CISSP – Qualys</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DHA/DoD Representative</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Event Description</td>
<td>Panel Moderator</td>
<td>Speaker</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 4:15pm-4:55pm| Overview of the NIST "Framework for Improving Critical Infrastructure Cybersecurity" | Panel Moderator: CDR Nikhil Thakur Regulatory Policy Advisor, EMCM / CDRH / FDA | Speaker:  
  - Kevin Stine – Manager of the Security Outreach & Integration Group, NIST |
| 4:55pm-5:05pm| Day 1 Recap, Set Stage for Day 2, Adjourn                                        | CDR Nikhil Thakur – EMCM / CDRH / FDA                                         |                                                                        |
### Agenda Day 2: October 22, 2014

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Presenter(s)</th>
<th>Moderator(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30am-9:00am</td>
<td>Registration</td>
<td>Suzanne Schwartz, MD, MBA – EMCM / CDRH / FDA</td>
<td></td>
</tr>
<tr>
<td>9:00am-9:05am</td>
<td>Welcome Remarks</td>
<td>Suzanne Schwartz, MD, MBA – EMCM / CDRH / FDA</td>
<td></td>
</tr>
<tr>
<td>9:05am-9:30am</td>
<td>Keynote Speaker</td>
<td>Michael Daniel, MS, MPP Special Assistant to the President and Cybersecurity Coordinator White House</td>
<td></td>
</tr>
<tr>
<td>9:30am-10:15am</td>
<td>Adapting and Implementing the NIST &quot;Framework for Improving Critical Infrastructure Cybersecurity&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Panel Moderator:</td>
<td>Debora Kobza, CGEIT, JIEM Executive Director NH-ISAC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Presenters:</td>
<td>• Kevin Stine – NIST</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Thad Odderstol, MS – Industry Engagement and Resilience, C³ Voluntary Program, OCS &amp; C / DHS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deborah Kobza, CGEIT, JIEM – NH-ISAC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Discussants:</td>
<td>• Kevin Hemsley, CISSP – ICS-CERT / DHS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Jeffery Goldthorp, MS – Associate Bureau Chief for Cybersecurity and Communications Reliability and Acting Chief of the Communications Systems Analysis Division in the Public Safety and Homeland Security Bureau, Federal Communications Commission (FCC)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deborah Kobza, CGEIT, JIEM – NH-ISAC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Thad Odderstol, MS – C³ Voluntary Program, OCS &amp; C / DHS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Kevin Stine – NIST</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CDRH Cybersecurity WG Representative / FDA</td>
<td></td>
</tr>
<tr>
<td>10:15am-11:30am</td>
<td>Adapting the Vision for Information Sharing and Shared Risk Assessment: Implementation within the HPH Sector</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Panel Moderator:</td>
<td>Margie Zuk, MS Senior Principal Cyber Security Engineer MITRE</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Session Description</td>
<td>Panel Moderator</td>
<td>Discussants</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>11:30am-1:00pm</td>
<td><strong>LUNCH</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00pm-1:10pm</td>
<td><strong>Keynote Speaker</strong></td>
<td>Mary Logan, JD, CAE</td>
<td>Steven Abrahamson, MBA – GE Healthcare</td>
</tr>
<tr>
<td></td>
<td></td>
<td>President and CEO</td>
<td>Mike Ahmadi, CISSP – Global Director of Medical Security, Codenomicon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Association for the Advancement</td>
<td>Steve Christey Coley – Principal Information Security Engineer in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>of Medical Instrumentation (AAMI)</td>
<td>Cyber Security Division, MITRE</td>
</tr>
<tr>
<td>1:10pm-2:40pm</td>
<td><strong>Development of Cybersecurity Tools, Risk Assessments, and Standards for the Healthcare and Public Health (HPH) Sector</strong></td>
<td>Ken Hoyme, MS</td>
<td>Ronald Mehring, MBA, CISSP – CISO-Senior Director of Information Security, Texas Health Resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distinguished Scientist</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adventium Labs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Co-chair Device Security Workgroup</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AAMI</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Section</td>
<td>Panel Moderator</td>
<td>Discussants</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2:40pm-2:55pm</td>
<td><strong>BREAK</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 2:55pm-4:50pm| **Building Potential Cybersecurity Solutions/Paths Forward for HPH**   | **Panel Moderator:** Dale Nordenberg, MD  
Executive Director Medical Device Innovation, Safety and Security Consortium (MDISS)  
CEO Novasano Health & Science | **Debra Bruemmer, MBA, CISSP – Mayo Clinic**  
**Steve Christey Coley – MITRE**  
**Rick Comeau, MBA – VP, Security Controls & Automation and Strategic Advisor to the CEO & President, Center for Internet Security (CIS)**  
**Sherman Eagles – Software CPR**  
**Thaddeus Flood, JD – MITA**  
**Kevin Fu, PhD – University of Michigan**  
**Ken Hoyme, MS – Adventium Labs/AAMI**  
**John Lu, MBA, MS, CISSP – Life Sciences Principal, Deloitte & Touche**  
**Michael McNeil, MBA – Philips Healthcare**  
**Ronald Mehring, MBA, CISSP – Texas Health Resources**  
**John Murray, MS – OC / CDRH /FDA**  
**Gavin O’Brien, MS – National Cybersecurity Center of Excellence (NCCoE) Project Manager, NIST**  
**Jeffrey Secunda, MS, MBA – AdvaMed**  
**Axel Wirth, MSc, CPHIMS, CISSP, HCISPP – Symantec** |
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>4:50pm-5:00pm</td>
<td><strong>Workshop Recap and Closing Remarks</strong></td>
<td>Suzanne Schwartz, MD, MBA, EMCM / CDRH / FDA</td>
</tr>
</tbody>
</table>
Cybersecurity Public Workshop Session Descriptions, Objectives, and Questions for Consideration

Day 1:

Welcome Remarks (9:00am-9:15am)
Suzanne Schwartz, MD, MBA
Director Emergency Preparedness/Operations and Medical Countermeasures Program (EMCM), Center for Devices and Radiological Health (CDRH) Food and Drug Administration (FDA)

Keynote Speaker (9:15am-9:30am)
Brigadier General Gregory Touhill (Invited)
Deputy Assistant Secretary for Cybersecurity Operations and Programs, Acting Director of National Cybersecurity and Communications Integration Center (NCCIC), Department of Homeland Security (DHS)

Session I (9:30am-11:00am) – Envisioning Collaboration for Medical Device and Healthcare Cybersecurity

Moderator: William Maisel, MD, MPH – FDA

Session Discussants:
Helen Caton-Peters, MSN, RN – Office of the National Coordinator for Health Information Technology (ONC) / Department of Health and Human Services
Stephen Curren, MS – Office of Emergency Management (OEM) / Assistant Secretary for Preparedness and Response (ASPR) / HHS
Rick Hampton – Partners Healthcare System
Lee Kim, JD, F HIMSS – Healthcare Information and Management Systems Society (HIMSS) North America
Carlos Kizzee (Invited), JD, LLM – Office of Cybersecurity and Communications (OCS&C) / DHS
Deborah Kobza, CGEIT, JIEM – National Healthcare Information Sharing and Analysis Center (NH-ISAC)
**Session I Information Sharing Objectives:**

1. Obtain input from the Sector on its information sharing needs
2. Describe characteristics of a collaborative information sharing environment
3. Provide examples of collaborative information sharing partnerships

**Questions for consideration:**

1. What are the benefits of establishing collaborative partnerships within the Sector?
2. What are the perceived impediments to creating a collaborative information-sharing environment? What are stakeholders’ concerns?
3. How can we establish partnerships within the HPH Sector to quickly identify, analyze, communicate, and mitigate cyber threats and medical device security vulnerabilities?
4. What should the federal government’s role be in addressing threats and vulnerabilities to medical devices?
5. As stakeholders, who should be included in the partnership?
6. What incentives are needed to spur collaboration?
   a. What incentives are needed to support proactive measures to strengthen cybersecurity?
7. Medical device vulnerability disclosures: who, what, when, and how?
   a. What if there’s a 0-day exploit discovered in the wild?
Session I - Shared Risk Assessment Framework Objectives:

1. Define shared risk
2. Describe characteristics of a shared risk assessment framework
3. Provide examples of shared risk assessment frameworks

Questions for consideration:

1. How might we encourage/facilitate acceptance of a shared ownership and shared responsibility model?
2. What are the challenges and benefits of a shared risk assessment framework?
3. What are the incentives needed to spur the development of a shared framework?
4. What are the possible roles?
5. What are the impediments?
6. What might a shared risk assessment framework look like?

BREAK (11:00am-11:15am)

Special Speaker (11:15am-11:25am)

Edward Gabriel, MPA, EMT-P, CEM, CBCP
Principal Deputy, Assistant Secretary of Preparedness and Response (ASPR)

Session II (11:25am-12:30pm) – Cyberthreat Landscape – Framing the Problem

Moderator: Steven Curren, MS – Division of Resilience and Infrastructure Coordination, OEM, ASPR
Session Presenters:

Marty Edwards – Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) / DHS
Jason Lay – Department of Health and Human Services (HHS)
Ray Strucker – Office of Criminal Investigation (OCI) / FDA

Session Discussants:

Terry Dunlap, MS – Tactical Network Solutions
Elisabeth George, MS – Philips Healthcare
Kevin Hemsley, CISSP – Idaho National Lab (INL) supporting ICS-CERT
Kevin McDonald, BSN, ME-PD, CISSP – Mayo Clinic
Billy Rios, MS, MBA, CISSP – Qualys
Wesley Snell, CISSP – Computer Security Incident Response Center (CSIRC) / HHS
CDR Nikhil Thakur – EMCM / CDRH / FDA
Axel Wirth, MSc, CPHIMS, CISSP, HCISPP – Symantec

Session II Objectives:

1. Discuss the current cyberthreat landscape both within and external to the healthcare and public health Sector (HPH)
2. Describe the current processes for identification, reporting, and communication of medical device vulnerability
3. Identify lessons learned from the threats themselves as well as the subsequent threat response
4. Identify the impact of the threats and incidents to the HPH Sector

Questions for consideration:

1. What type of cyber threats and vulnerabilities are we seeing?
   a. What are the motivations behind these?
2. Are there threats that are unique to the HPH Sector?
3. What is the degree of awareness of these threats within the sector?

4. How well-positioned is HPH to address these threats? Does it vary across the sector? What needs to change?“

5. How are organizations currently processing threat information?
   a. Do organizations think they are receiving useful/actionable information?

6. How can threat models (within and outside the sector) help to mitigate safety concerns?

7. What lessons have been learned from responding to cyberthreats within and external to the HPH Sector?

8. Given current processes for reporting vulnerabilities in HPH, what happens if the communication between researcher and manufacturer/vendor break down?

LUNCH (12:30pm-1:40pm)

[Session III] (1:40pm-2:30pm) – Cybersecurity Gaps and Challenges: Need to Share vs. Need to Secure

Moderator: Julian Goldman, MD – Partners Healthcare System & Massachusetts General Hospital

Session Discussants:

Sherman Eagles – Software CPR
Ramya Krishnan, MS – Health Devices Group, ECRI Institute
Darren Lacey, JD – Johns Hopkins University/Johns Hopkins Medicine
Jackie McCarthy, JD – CTIA-The Wireless Association®
Linda Ricci – Cardiac Diagnostic Devices / Office of Device Evaluation (ODE) / CDRH / FDA
Billy Rios, MS, MBA, CISSP – Qualys
Jeffrey Secunda, MS, MBA – AdvaMed
DHA/DoD Representative
Session III Objectives:

1. Discuss gaps and challenges concerning interconnectivity across the HPH ecosystem
2. Discuss how the interconnectivity of devices and systems increases exposure to cyberthreats and how that exposure affects the safe use of medical devices.
3. Discuss ways to balance the need to share/secure information

Questions for consideration:

1. Is device interoperability and information sharing an either/or situation?
2. Do the discussants think networks adequately isolate and contain compromised systems? Why or why not?
3. How do you strike the balance between the inevitable need for device interconnectivity versus the need to secure the information they are relaying?

Session IV (2:30pm-3:15pm) – Cybersecurity Gaps and Challenges: Legacy Devices

Moderator: Kevin Fu, PhD – Archimedes Center for Medical Device Security, University of Michigan

Session Discussants:

Steven Abrahamson, MBA – Product Security Engineering, GE Healthcare
Penny Chase, MS, MA – Information Technology Technical Center, MITRE
Josh Emperado, MS – Toshiba America Medical Systems & Medical Imaging and Technology Alliance (MITA)
Brian Fitzgerald – Office of Science and Engineering Labs (OSEL) / CDRH /FDA
Thaddeus Flood, JD – MITA
Elisabeth George, MS – Philips Healthcare
Darren Lacey, JD – Johns Hopkins University/Johns Hopkins Medicine
John Murray, MS – Office of Compliance (OC) / CDRH /FDA
Jay Radcliffe, MS, CISSP – Rapid7
**Session IV Objectives:**

1. Gain an enhanced perspective as to the magnitude of legacy device usage
2. Gain diverse perspectives on gaps and challenges concerning legacy devices across the HPH ecosystem
3. Develop an enhanced understanding of the threats and vulnerabilities encountered on legacy devices
4. Develop an understanding of how organizations are attempting to secure these devices, and whether these approaches are working

**Questions for consideration:**

1. Are there threats and vulnerabilities that are unique to legacy devices? If so, what are they?
2. How have stakeholders responded to these threats and vulnerabilities?
   a. How could a shared framework of knowledge and responsibility improve the response to threats and vulnerabilities?
3. Can legacy device use be curtailed/phased out? Is this a viable goal? What impediments exist?”
4. Who is responsible for patching? What happens when a legacy device is no longer supported?
5. Who should be responsible for securely configuring the device? How can this process be improved?

**BREAK (3:15pm-3:30pm)**

**Session V (3:30pm-4:15pm) – Cybersecurity Gaps and Challenges: Forward Looking Design**

**Moderator:** Thaddeus Flood, JD – MITA
**Session Discussants:**

Bill Aerts, CISSP, CISM – Global Privacy and Security Office, Medtronic
Debra Bruemmer, MBA, CISSP – Mayo Clinic
Abiy Desta – ODE / CDRH / FDA
Ken Hoyme, MS – Adventium Labs & Advancement of Medical Instrumentation (AAMI)
Darren Lacey, JD – Johns Hopkins University/Johns Hopkins Medicine
Michael McNeil, MBA – Global Product Security and Services, Philips Healthcare
Billy Rios, MS, MBA, CISSP – Qualys
DHA/DoD Representative

**Session VI Objectives:**

1. Increase awareness of the gaps and challenges encountered in designing cybersecurity resiliency into medical devices
2. Develop an enhanced understanding of how threats and vulnerabilities may be mitigated using already established and potentially new product design principles and methodologies

**Questions for consideration:**

1. Are manufacturers adapting current product design principles to address cybersecurity concerns or do they anticipate inventing new design methodologies to enhance product cybersecurity??
2. What challenges are encountered in trying to incorporate cybersecurity into medical device design? What knowledge gaps exist regarding the incorporation of cybersecurity into medical device design? Can these knowledge gaps be addressed in a collaborative environment?
3. How can resilience to future threats and vulnerabilities be realized proactively via prospective design?
4. If a vulnerability is exploited, how will cyber resiliency and recovery be achieved? What might incident response planning for an intrusion, exploit or data breach look like for all stakeholders?

5. Is using more secure development methods/design of embedded systems within medical devices a realistic goal? What are the impediments?

6. Is there anything we can learn from other industries/sectors (e.g. industrial control systems)

7. Is there a role for health care entity/vendor contractual measures that stipulate use of secure development techniques, including a plan for ongoing support (e.g., delivery of security updates and patches) or other security measures?

8. Should prospective design be restricted to individual devices or is it also necessary to better architect the entire networked environment?

**Session VI (4:15pm-4:55pm) – Overview of the NIST “Framework for Improving Critical Infrastructure Cybersecurity”**

**Moderator:** CDR Nikhil Thakur – EMCM /CDRH / FDA

**Session Speaker:**

Kevin Stine – Security Outreach & Integration Group NIST

**Session VI Objectives:**

1. Increase awareness of the “Framework for Improving Critical Infrastructure Cybersecurity”

2. Highlight key components of “The Framework”

3. Discuss the implementation of “The Framework” within the context of Executive Order 13636’s emphasis on voluntary mechanisms
Questions for consideration:

1. What is “The Framework”?

2. How might “The Framework” be leveraged for use across Sectors and organizations?

3. Is there a regulatory role in the implementation of the framework? If so what is it?

Day 1 Recap (4:55pm-5:10pm)

CDR Nikhil Thakur – EMCM /CDRH / FDA
Day 2:

Welcome Remarks (9:00am-9:05am)

Suzanne Schwartz, MD, MBA – EMCM / CDRH / FDA

Keynote Speaker (9:05am-9:30am)

Michael Daniel, MS, MPP
Special Assistant to the President and Cybersecurity Coordinator, White House

Session VII (9:30am-10:15am) – Adapting and Implementing the NIST "Framework for Improving Critical Infrastructure Cybersecurity"

Moderator: Deborah Kobza, CGEIT, JIEM – NH-ISAC

Session Presenters:

Kevin Stine – NIST
Thad Odderstol, MS – C³ Voluntary Program, OCS & C / DHS
Deborah Kobza, CGEIT, JIEM – NH-ISAC

Session Discussants:

Kevin Hemsley, CISSP – ICS-CERT / DHS
Jeffery Goldthorp, MS – Cybersecurity and Communications Reliability & Communications Systems Analysis Division, Public Safety and Homeland Security Bureau, Federal Communications Commission (FCC)
Deborah Kobza, CGEIT, JIEM – NH-ISAC
Thad Odderstol, MS – C³ Voluntary Program, OCS & C / DHS
Kevin Stine – NIST
CDRH Cybersecurity WG Representative – FDA
**Session Objectives:**

1. Describe how “The Framework” has been adapted and implemented across organizations and Sectors
2. Discuss how “The Framework” might be adapted and implemented across the HPH Sector

**Questions for consideration:**

1. How has “The Framework” been adapted and implemented within and external to the HPH Sector?
2. What unique challenges exist for the adaptation and implementation of “The Framework” for medical device cybersecurity and how might these be addressed?
3. What are the roles and responsibilities of various stakeholders within the Sector in the adaptation and implementation of “The Framework” for medical device cybersecurity?
4. Will the application of the framework vary across the HPH sector? If so, how? Is that appropriate?”
5. How can the framework help organizations at various levels of maturity in the vulnerability management of medical devices?

**Session VIII** (10:15am-11:30am) – *Adapting the Vision for Information Sharing and Shared Risk Assessment: Implementation within the HPH Sector*

**Moderator:** Margie Zuk, MS – MITRE

**Session Discussants:**

Bill Aerts, CISSP, CISM – Medtronic
Penny Chase, MS, MA – Information Technology Technical Center, MITRE
Rick Hampton – Partners Healthcare System
Deborah Kobza, CGEIT, JIEM – NH-ISAC
Michael Frederick, MS, CISSP – Assurance Services and Product Development, HITRUST
Bakul Patel, MS, MBA – CDRH / FDA
CDR Nikhil Thakur – EMCM / CDRH / FDA
Axel Wirth, MSc, CPHIMS, CISSP, HCISPP – Symantec

**Session VIII Objectives:**

1. Discuss the roles and responsibilities of the various stakeholders within this information sharing environment
2. Discuss the roles and responsibilities of the various stakeholders within this shared risk assessment framework
3. Discuss approaches to operationalizing information sharing and shared risk assessment

**Questions for consideration:**

1. What information sharing models and security risk assessment frameworks exist?
2. How have other Sectors leveraged information sharing to enhance cybersecurity?
3. How might we create incentives to encourage sharing of cyber threats and vulnerabilities?
4. What are the roles and responsibilities of various stakeholders within the Sector regarding information sharing and shared risk assessment?
5. How might we create a shared risk assessment framework and what would this look like?
6. What information with regard to medical device security should be shared?

**LUNCH (11:30am-1:00pm)**

**Special Speaker (1:00pm-1:10pm)**

Mary Logan, JD, CAE
President and CEO, Association for the Advancement of Medical Instrumentation (AAMI)
Session IX (1:10pm-2:40pm) – Development of Cybersecurity Tools, Risk Assessments, and Standards for the Healthcare and Public Health Sector

**Moderator:** Ken Hoyme, MS – Adventium Labs & AAMI

**Session Discussants:**

Steven Abrahamson, MBA – GE Healthcare
Mike Ahmadi, CISSP – Medical Security, Codenomicon
Steve Christey Coley – Cyber Security Division, MITRE
Brian Fitzgerald – OSEL / CDRH / FDA
Deborah Kobza, CGEIT, JIEM – NH-ISAC
Ronald Mehring, MBA, CISSP – Texas Health Resources
Bryan Cline, PhD, CISSP-ISSEP, CISM, CISA, ASEP, CCSFP, HCISPP – HITRUST
Henri “Rik” Primo, MS – SYNGO (Imaging Informatics) Division, Siemens Medical Solutions USA

**Session IX Objectives:**

1. Discuss the cybersecurity tools currently available and those in development
2. Discuss current cybersecurity standards and those in development
3. Discuss the risk assessments currently performed and those in development
4. Ideate about the critical components needed for cybersecurity tools, standards, and risk assessment for the HPH Sector

**Questions for consideration:**

1. From the HPH perspective, what critical components/factors should be incorporated into:
   a. cybersecurity tools
   b. cybersecurity standards
   c. cybersecurity risk assessment
2. What are the roles and responsibilities of various stakeholders in the development of tools, risk assessments, and standards?

3. What are some examples of recent or upcoming standards, tools or risk assessments?
   a. What are potential barriers to their adoption (e.g. costs, personnel resources, etc.)?

How might these be addressed?

BREAK (2:40pm-2:55pm)

Session X (2:55pm-4:50pm) – Building Potential Cybersecurity Solutions/Paths Forward for HPH

Moderator: Dale Nordenberg, MD – Medical Device Innovation, Safety and Security Consortium (MDISS) & Novasano Health & Science

Session Discussants:
Debra Bruemmer, MBA, CISSP – Mayo Clinic
Steve Christey Coley – MITRE
Rick Comeau, MBA – Center for Internet Security (CIS)
Sherman Eagles – Software CPR
Thaddeus Flood, JD – MITA
Kevin Fu, PhD – Archimedes Center for Medical Device, University of Michigan
Ken Hoyme, MS – Adventium Labs & AAMI
John Lu, MBA, MS, CISSP – Deloitte & Touche
Michael McNeil, MBA – Global Product Security and Services, Philips Healthcare
Ronald Mehring, MBA, CISSP – Texas Health Resources
John Murray, MS – OC / CDRH /FDA
Gavin O’Brien, MS – National Cybersecurity Center of Excellence (NCCoE), NIST
Jeffrey Secunda, MS, MBA – AdvaMed
Axel Wirth, MSc, CPHIMS, CISSP, HCISPP – Symantec
Timothy Skutt – Wind River Systems
DHA/DoD Representative
**Session X Objectives:**

1. Discuss the FDA’s current thinking on its involvement in the cybersecurity of medical devices
2. Discuss tangible next steps for the HPH sector including roles and responsibilities of the various stakeholders
3. Provide examples of ongoing work and projects in development to address cybersecurity of medical devices

**Questions for consideration:**

1. How does the FDA’s recently finalized premarket guidance fit in with some of the current initiatives underway in the sector
2. What role should the FDA (or broader government) have in these initiatives?
3. What additional measures can FDA be taking to further support the advancement of medical device cybersecurity?
4. What changes tomorrow: next steps for public/private entities working collaboratively in addressing the challenges in medical device and healthcare cybersecurity?

**Workshop Recap (4:50pm-5:00pm)**

Suzanne Schwartz, MD, MBA, EMCM / CDRH / FDA
Steve Abrahamson, MBA
Director of Product Security Engineering
GE Healthcare
Steven.Abrahamson@med.ge.com

Steve Abrahamson, Director of Product Security Engineering at GE Healthcare, is leading the development and implementation of Medical Device Cyber Security and Privacy across all GE Healthcare product lines. This includes establishing new design standards and engineering practices through collaboration with technical experts, commercial organizations, customers, design teams, and industry groups. Steve is engaged in promoting a collaborative approach for healthcare security as a frequent speaker at events including the US Information Security and Privacy Advisory Board, National Academy of Sciences, HHS/NIST HIPAA Security Conference, HIMSS, mHealth, MDM East, and the SANS Healthcare Cyber Security Summit. Steve is a certified Six Sigma Black Belt and Master Black Belt, and has a Bachelor’s Degree in Mechanical Engineering from Marquette University and a MBA from the University of Dallas. Steve works at GEHC’s offices in his hometown of Waukesha, Wisconsin.
Bill Aerts, CISSP, CISM
Director of Information and Product Security
Medtronic’s Global Privacy and Security Office
bill.aerts@medtronic.com

Bill Aerts is the Director of Information and Product Security within Medtronic’s Global Privacy and Security Office. In this role, Bill oversees Information Security, Disaster Recovery, and the corporate Product Security Program. He has created and championed information and product security programs in the insurance, transportation, retail and healthcare industries throughout his career. His primary focus currently is on the Global Product Security program, which brings together the product R&D functions throughout the Company to improve focus on security, integrate security into the product development lifecycle, monitor industry and regulatory trends, represent Medtronic on product security matters in the public setting, and provide other security services to the business.

Bill received his bachelor’s degree from the University of Wisconsin, and holds CISSP and CISM certifications.
Mike Ahmadi, CISSP
Global Director of Medical Security Codenomicom

The objective of Codenomicom is to ensure the security and robustness of any application or service implementation. Mike has extensive background in both Project Management and Information Systems for projects addressing cyber security in multiple vertical industries, including energy, industrial automation, and health care.

Mike currently serves as a member of the Medical Device Innovation, Safety, and Security Consortium (MDISS) and is a member of the Association for the Advancement of Medical Instrumentation (AAMI) Medical Device Security Working Group and Wireless Strategy Task Force. He is also a designated IEC US Expert for TC65 WG10, where he is currently serving with other IEC experts in creating the IEC 62443 series of standards. Mike is also currently serving on the US Secret Service Electronic Crimes Task (USSS ECTF) Advisory Board, and is currently assisting the FDA in the creation of the FDA Cybersecurity Testing Lab.
Debra Bruemmer is a Principle Information Security Analyst at Mayo Clinic in Rochester, Minnesota. She works in Clinical Information Security in the Office of Information Security. Debra received her Bachelor of Science in Finance from Winona State University, a Masters in Business Administration from Cardinal Stritch University, and is CISSP certified. Her primary focus is on Clinical Information Security and assessing and improving the security of medical devices. Her responsibilities include, understanding medical devices in the Mayo Clinic environment, assessing the vulnerability of medical devices, and partnering with vendors and internal staff to improve security. During her fifteen-year career at Mayo Clinic, Debra has worked in Finance, Information Technology, and the Office of Information Security.
Helen Caton-Peters MSN, RN
Health IT Privacy and Security Specialist
Office of the Chief Privacy Officer
Office of the National Coordinator
Helen.Caton-Peters@hhs.gov

Helen Caton-Peters MSN, RN works as a Health IT Privacy and Security Specialist in the Office of the Chief Privacy Officer in the Office of the National Coordinator. In that role, she advises the National Coordinator on health information privacy, security, and data stewardship policy efforts related to electronic health information. Since joining HHS in 2013, Ms. Caton-Peters has worked collaboratively with the HHS Office for Civil Rights (OCR) and other divisions of HHS, other Federal agencies, State and regional programs, and other countries to help ensure a coordinated approach to maintaining the privacy and security of electronic health information. She has over 20 years’ nursing experience in clinical, education, informatics, and policy positions. As a Clinical Nurse Specialist she has experience in high-risk OB/GYN and Pediatrics and several combined years’ experience teaching nursing as a clinical and classroom instructor. As a Nurse Informaticist she has worked to advance adoption of Health IT for over 15 years by facilitating and leading clinical and technical teams in EHR implementation and clinical transformation efforts while maintaining a strong focus on privacy and security of health information and patient rights. Ms. Caton-Peters holds a Master’s of Science in Nursing Degree from The Medical University of South Carolina and a Bachelors of Science in Nursing Degree in Nursing from Binghamton University in New York State.
Penny Chase is the Information Technology and Cyber Security Integrator in the Information Technology Technical Center at The MITRE Corporation. In this role Penny promotes collaboration across MITRE’s Information Technology and Cyber Security Technical Centers. Previously she was the Department Head for Human Language Technology within the Information Technology Technical Center. She has led MITRE and government-sponsored projects in developing structured representations for malware and threat information, security visualization, software assurance, malware analysis, reverse engineering, software architecture and design pattern recovery, network penetration testing, legacy database encapsulation, machine learning, and discourse-based natural language interfaces. Penny’s research has been presented at dozens of conferences.

Penny is the Principal Investigator of a MITRE Sponsored Research Project on medical device security and safety, and supports MITRE’s FDA/CDRH project on medical device cybersecurity. She also leads the DHS Malware Attribute Enumeration and Characterization (MAEC) project for DHS. Previously Penny chaired the DHS/DOD/NIST Software Assurance Forum Working Group on Malware; served as the Deputy Director of the ARDA Northeast Regional Research Center, managing workshops that addressed Intelligence Community challenge problems; and was a member of the NASA Advisory Council’s subcommittee on Avionics, Software, and Cybersecurity.

Penny received her Bachelor of Arts in Mathematics and History (with Harpur College Honors) from the State University of New York at Binghamton in 1975. She received her Master of Arts in the History of Science from Harvard University in 1976 and her Master of Science in Computer Science from Harvard University in 1986.
Steve Christey Coley is a Principal Information Security Engineer in the Cyber Security Division at The MITRE Corporation, supporting the FDA CDRH on Medical Device Cyber Security. He likes changing his last name every two decades or so. Steve is the co-creator and Editor of the Common Vulnerabilities and Exposures (CVE) list, chair of the CVE Editorial Board since 1999, and the technical lead for the Common Weakness Enumeration (CWE), Common Weakness Scoring System (CWSS), and the community-driven CWE/SANS Top 25 Software Most Dangerous Software Errors. He is a co-author of the influential "Responsible Vulnerability Disclosure Process" IETF draft with Chris Wysopal in 2002. He was an active contributor to other efforts including the Common Vulnerability Scoring System (CVSS), the Common Vulnerability Reporting Framework (CVRF), NIST's Static Analysis Tool Exposition (SATE) and certain non-public projects involving the assessment of static code analysis tools, and the SANS Secure Programming exams. His current interests include exploring analogies between epidemiology and information security (such as bias in vulnerability statistics and research); ensuring that emerging technologies do not repeat the chaotic path to effective vulnerability management that occurred with enterprise software in the 1990s; secure software development and testing; consumer-friendly software security metrics; the theoretical underpinnings of vulnerabilities; improving the exchange of vulnerability information on an international level; and making the computer security profession accessible to everybody who seeks a place in it. He holds a B.S. in Computer Science from Hobart College.
Bryan Cline, PhD, CISSP-ISSEP, CISM, CISA, ASEP, CCSFP, HCISPP
Senior Advisor to the Health Information Trust Alliance (HITRUST)

Bryan Cline, PhD, CISSP-ISSEP, CISM, CISA, ASEP, CCSFP, HCISPP, as a Senior Advisor to the Health Information Trust Alliance (HITRUST), Frisco, TX, provides thought leadership for the continuing development and implementation of the HITRUST Common Security Framework (CSF), the healthcare industry’s de facto information protection standard. Previously the VP of CSF Development and Implementation, Dr. Cline helped mature the CSF and CSF Assurance Program as part of a more comprehensive risk management framework—a model implementation of the national Framework for Critical Infrastructure Cybersecurity for healthcare; spearheaded development of the Texas Covered Entity Privacy and Security Certification program—the first state-recognized certification of its kind; and partnered with (ISC)2 to create the Health Care Information Security and Privacy Practitioner (HCISPP) credential—a gold standard entry-level certification specifically for health information protection professionals. Dr. Cline also served as the Chief Information Security Officer (CISO) and Director of Information Security at Catholic Health East, Newtown Square, PA, a large faith-based healthcare system, and CISO and Director of Information Security Risk Management at The Children’s Hospital of Philadelphia, PA, a leading pediatric research hospital. It was at Children’s when he first began working with the CSF and became one of HITRUST’s most vocal advocates. Over the past seven years, Bryan has presented on the subject of organizational-level CSF implementation and risk management at SC World Congress, SecureWorld Expo, and other forums. But it was at CHE where Dr. Cline garnered the 2010 HITRUST Award for Security and Privacy Practices. Bryan holds a Doctorate in information systems with a concentration in information assurance policy from the University of Fairfax, Vienna, VA, a Master of Science degree in industrial engineering with a concentration in operations research from the University of Oklahoma, Norman, and a Baccalaureate in mathematics from the University of Texas at Arlington.
Rick Comeau, MBA
Strategic Advisor to the Center for Internet Security’s (CIS) CEO & President
Center for Internet Security
rick.comeau@cisecurity.org

Rick Comeau serves as Strategic Advisor to the Center for Internet Security’s (CIS) CEO & President and is responsible for assisting with planning and implementing the strategic direction of CIS. Rick is also the Vice President of CIS’s Security Controls and Automation (SCA) business unit. SCA helps to improve both private and public sector organizations’ cyber security posture by helping them reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. SCA provides enterprises with consensus-based, best practice standards for system security configurations (“CIS Benchmarks”), as well as automated resources for measuring information system security status and for making informed decisions on security investments.

Before joining CIS, Rick was the Assistant Deputy Director for Strategic Planning & Administration at the New York State Office of Cyber Security and Critical Infrastructure Coordination, where he assisted senior leadership on a variety of planning, policy and budgetary activities. Before working in New York State government, Rick was a management consultant supporting several federal departments and agencies, including the U.S. Department of Homeland Security, the Federal Bureau of Investigation, the National Security Agency and the U.S. Department of Energy.

Prior to his time as a consultant, Rick spent several years as an officer in the U.S. Coast Guard, serving as Communications Officer and Deck Watch Officer on a High Endurance Cutter performing patrols to enforce fisheries laws and treaties and conduct search and rescue missions. He next led a specialized interdiction team to counter seaborne drug smuggling. His final tour was spent helping to financially sustain the Coast Guard’s fleet of cutters and their numerous, critical operations. Rick earned a Master of Business Administration degree from the George Washington University and received an undergraduate degree from the U.S. Coast Guard Academy.
Stephen Curren, MS
Acting Director of the Division of Resilience and Infrastructure Coordination
Within this Division is the Critical Infrastructure Protection Program
Office of Assistant Secretary for Preparedness and Response
U.S. Department of Health and Human Services (HHS)

Steve Curren is Acting Director of the Division of Resilience and Infrastructure Coordination in the Office of Assistant Secretary for Preparedness and Response at the U.S. Department of Health and Human Services (HHS). Within this Division is the Critical Infrastructure Protection Program, which focuses on partnership with private sector, state, and local organizations to mitigate risks to the Healthcare and Public Health Sector from all hazards. It operates under the National Infrastructure Protection Plan on a framework based on voluntary partnership, risk analysis, and information sharing. The partners engaged in this effort with HHS encompass all aspects of the Healthcare and Public Health Sector, including direct patient healthcare, health plans and payers, pharmaceuticals, laboratories, blood supply, medical materials, health information technology, mortuary care, and governmental public health.

Steve arrived at HHS in 2008 after working five years at the Association of State and Territorial Health Officials (ASTHO), where he served as Senior Director for Public Health Preparedness. In this capacity he directed a program to develop and disseminate model policies and practices to advance public health preparedness for state and territorial public health agencies. Prior to joining ASTHO he served for four years as an industry consultant on U.S. and European public health and regulatory policy issues. He holds a Bachelor of Science degree in Biology from Wake Forest University and Master of Science degree in International Business-Government Relations from the Georgetown University Walsh School of Foreign Service.
Michael Daniel, MS, MPP
Special Assistant to the President and Cybersecurity Coordinator

Michael Daniel is a Special Assistant to the President and the Cybersecurity Coordinator. In this position, Michael leads the interagency development of national cybersecurity strategy and policy, and he oversees agencies’ implementation of those policies. Michael also ensures that the federal government is effectively partnering with the private sector, non-governmental organizations, other branches and levels of government, and other nations.

Prior to coming to the National Security Staff, Michael served for 17 years with the Office of Management and Budget (OMB). From September 2001 to June 2012, he served as the Chief of the Intelligence Branch, National Security Division, in a career Senior Executive Service position. This branch oversees the Intelligence Community (IC) and other classified Department of Defense programs. In this position, Michael played a key role in shaping intelligence budgets, improving the management of the IC, and resolving major IC policy issues. The branch also oversaw a variety of cross-cutting issues, including cybersecurity, counterterrorism spending, and information sharing and safeguarding.

Within OMB, Michael also served as an examiner in the National Security Division’s Front Office supporting the Deputy Associate Director and in the Operations branch reviewing Navy and Marine Corps operational activities and overseas military operations such as Bosnia and Kosovo.

Since 2007, Michael has been heavily involved with Federal cybersecurity activities, starting with the Comprehensive National Cybersecurity Initiative. He has worked on cybersecurity funding issues in almost every budget since then and led an annual cross-cut review of Federal agencies’ cybersecurity spending. He represented OMB on cybersecurity issues in the interagency policy process and worked with various Congressional committees and staff on cybersecurity issues. Finally, he has worked on tracking cybersecurity spending and the development of useful cyber performance metrics.

Originally from Atlanta, Michael received a Bachelor’s in Public Policy from the Woodrow Wilson School at Princeton University. Subsequently, he obtained a Master’s in Public Policy from the Kennedy School of Government at Harvard with a focus on International Affairs and Security. Michael also obtained a Master of Science in National Resource Strategy from the National Defense University’s Industrial College of the Armed Forces in 2001.

Outside of work, Michael and his wife are raising two rambunctious boys. Michael also studies martial arts in the Chishin Ryu style with Dai Nippon Botoku Kai, a Norfolk-based karate association.
Sherman was a Technical Fellow at Medtronic before his retirement in 2008. He has over 40 years of software experience, including development work on operating systems, communications systems, software development tools and software development processes. In eighteen years at Medtronic, he focused on software process, software safety and software reliability in medical devices. Sherman is now providing assistance to the Center for Medical Interoperability and is a Partner at SoftwareCPR, a consulting group specializing in regulated medical software.

Sherman is a co-chair of the Medical Device Software Working Group of AAMI, and a co-author of the AAMI manual, “Getting Started with IEC 80001-1: Essential Information for Healthcare Providers Managing Medical IT-Networks. He developed and is the lead instructor for the AAMI course on Safety Assurance Cases for Medical Devices. He has also developed and taught courses on Software risk management and Software Standards for medical device regulations. He was the convener and editor for international standard IEC 62304 on medical device software life cycle processes, and the convener of the working group that developed IEC 80002-1 on application of ISO 14971 risk management for medical device software. He is currently the co-convener of the international standards group on risk management for IT networks that include medical devices and was the editor of IEC 80001-1. He also is the convener of the IEC Maintenance Team for the safety requirements for programmable electrical medical systems (PEMS) in IEC 60601-1.

Sherman is a past chair of the AdvaMed device software working group, served on the technical advisory committee of the Software Productivity Consortium, and was a member of the ad-hoc Software Committee of the Global Harmonization Task Force.

Sherman received a Bachelor’s degree in physics from Macalester College in 1968.
Marty Edwards
Assistant Deputy Director,
National Cybersecurity and Communications Integration Center (NCCIC)
Director,
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
Department of Homeland Security
ics-cert@dhs.gov

Marty Edwards is the Director of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), an operational division of the department’s National Cybersecurity and Communications Integration Center (NCCIC) and the DHS Office of Cybersecurity and Communications (CS&C).

ICS-CERT works to reduce industrial control system risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local and tribal governments, as well as industrial control systems owners, operators and vendors. In collaboration with the other NCCIC components the ICS-CERT responds to and analyzes control systems related incidents, conducts vulnerability and malware analysis, and shares and coordinates vulnerability information and threat analysis through products and alerts.

Mr. Edwards has over 20 years of experience and brings a strong industrial control system industry focus to DHS. Before coming to the ICS-CERT, Mr. Edwards was a program manager focused on control systems security work at Idaho National Laboratory. Prior to his work at the laboratory, Mr. Edwards held a wide variety of roles in the instrumentation and automation fields, including field service, instrument engineering, control systems engineering and project management.

Mr. Edwards has also held various positions in nonprofit organizations, including Chairman of the Board for one of the automation communities’ largest user group conferences. Mr. Edwards holds a diploma of technology in Process Control and Industrial Automation (Magna cum Laude) from the British Columbia Institute of Technology.

The ICS-CERT is the recipient of the 2013 SC Magazine Security Team of the Year award.
Joshua “Josh” Emperado, MSBME, MSEE
Sr Manager, Market Development MR
Toshiba America Medical Systems

Josh Emperado is a veteran of the medical imaging industry with over 15 years of experience. Throughout his career, Josh has been focused on the workflow and connectivity needs of customers in Radiology and Cardiology. He has a vast background in the development, implementation, support and marketing of medical imaging products. At each company, Josh has been involved in guiding development, regulatory and marketing groups on Imaging Informatics standards, policies and emerging technologies.

Currently, Josh Emperado is responsible for MR Market Development for Toshiba America Medical Systems. Josh concentrates his efforts on understanding the patient workflow in MR from acquisition to reading. Prior to Toshiba, Josh worked at Philips Healthcare in Global Marketing for Enterprise Advanced Visualization. Before that, he held the role of product manager, Radiology PACS, at Siemens Healthcare’s SYNGO Americas Division. At both Philips and Siemens, Josh managed multiple product launches and was involved in other multi-modality work including research, engineering, consulting and marketing.

Josh is currently the Vice Chair of the Medical Imaging Informatics Section of the Medical Imaging Technology Alliance (MITA).

Josh holds a Master of Science in Biomedical Engineering and Master of Science in Electrical and Computing Engineering from Drexel University, having done his Master’s research in MR Physics. He has also has a Bachelors of Science in Mechanical Engineering from the University of Maryland Baltimore County.

Josh resides in Anaheim Hills CA with his wife Valerie and two children, Zoe and Jude.
Thaddeus Flood, JD
Industry Director for X-Ray and Medical Imaging Informatics
MITA

Thaddeus Flood is MITA’s Industry Director for X-Ray and Medical Imaging Informatics. Prior to joining MITA, Thaddeus served as a Project Officer with the United States Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, where he oversaw state health information exchange grants and encouraged adoption of meaningful use standards among eligible healthcare providers. He has a background and interest in healthcare policy and regulatory matters. Thaddeus earned a BA in International Political Economy from Fordham University, and a Juris Doctor, cum laude, from the American University Washington College of Law.
Michael Frederick, MS
Vice President of Assurance Services and Product Development
HITRUST.

Michael Frederick has 20+ years experience in information security. He is currently the Vice President of Assurance Services and Product Development at HITRUST. Prior to joining HITRUST he was CEO of The Frederick Group, a professional services firm focused on security risk management in healthcare. He served as Chief Information Security Officer (CISO) for eight years at a large healthcare system. While in this role, he led the organization in becoming the first hospital system to be certified under the HITRUST Common Security Framework™ (CSF) and was the industry lead in the provider space during the development of the CSF. He has been a speaker at numerous security events and has been published on the topics of risk management, applying security practices within an organization, and how to build an effective security organization. Prior to his CISO role, he was a security architect, security manager in industry and a security consultant in various large accounting firms. He has been a Certified Information System Security Professional (CISSP) since 1999.
Kevin Fu is Associate Professor of Electrical Engineering and Computer Science at the University of Michigan where he directs the Archimedes Center for Medical Device Security and the SPQR.eecs.umich.edu research group. His research investigates how to achieve trustworthy computing on embedded devices with application to health care, commerce, and communication. His team’s provocative 2008 research paper analyzing the security of a pacemaker/defibrillator led to a watershed moment in cybersecurity for medical device manufacturing and regulatory science.

Prof. Fu received his Ph.D. in EECS from MIT where his doctoral research pertained to secure storage and web authentication. Fu received a Sloan Research Fellowship, NSF CAREER award, Fed100 Award, and best paper awards from various academic silos of computing. The research is featured in critical articles by the NYT, WSJ, and NPR. Kevin was named MIT Technology Review TR35 Innovator of the Year for work on medical device security. Kevin has testified in Congress on health matters and has written commissioned work for the Institute of Medicine of the National Academies. He served as a visiting scientist at the Food & Drug Administration, the Beth Israel Deaconess Medical Center of Harvard Medical School, Microsoft Research, and MIT CSAIL. Previous employers include Bellcore, Cisco Systems, HP Labs, and Holland Community Hospital. He is a member of the ACM Committee on Computers and Public Policy and the NIST Information Security and Privacy Advisory Board. He is a principal investigator of THaW.org. Prior to joining Michigan, he served on the faculty at UMass Amherst. Kevin also holds a certificate of achievement in artisanal bread making from the French Culinary Institute.
Edward J. Gabriel, MPA, EMT-P, CEM, CBCP
Principal Deputy Assistant Secretary for Preparedness and Response
Department of Health and Human Services

Mr. Gabriel is the Principal Deputy Assistant Secretary for Preparedness and Response. In this role, he serves as principal advisor to the Assistant Secretary for Preparedness and Response (ASPR) on all matters pertaining to and in support of the Department’s public health emergency preparedness and response and recovery activities, programs, and policies. Mr. Gabriel provides strategic oversight to the organization with an emphasis on enhancing state and local preparedness, policies and plans relating to public health and medical emergencies, emergency response operations, financial analysis and advanced development of and manufacturing of critical medical countermeasures for man-made and naturally occurring public health threats.

Prior to joining ASPR, he served as Director, Global Crisis Management and Business Continuity, for The Walt Disney Company. He was responsible for the development and implementation of global policy, planning, training and exercises to manage crisis, provided leadership and direction to east and west coast medical and emergency medical operations, the Walt Disney Studio’s fire department and provided crisis support with global business units. During Crisis incidents his department managed response operations, communications methodology and disaster and business recovery.

Preceding this private sector position, Mr. Gabriel held positions in New York City. He was a twenty-six year Paramedic veteran of New York City Fire Department’s (FDNY) Emergency Medical Service (EMS) retiring as an Assistant Chief/Division Commander. He was assigned to New York City Office of Emergency Management (NYC*OEM) as Deputy Commissioner for Planning and Preparedness and was responsible for all preparedness and planning-related strategy, projects and initiatives until he retired from NYC Government.

Mr. Gabriel has served on several National Academy of Sciences – Institute of Medicine (NAS-IOM) committees including Chair of the Standing Committee for the Department of Homeland Security (DHS) on Health Threats Resilience, and IOM Committee on Crisis Standards of Care and the Disaster Resource Guide Editorial Board. He currently serves on the Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), National Advisory Council (NAC). Additionally he served on the Centers for Disease Control (CDC) – Board of Scientific Counselors for the Coordinating Office for Terrorism Preparedness and Emergency Response.

Mr. Gabriel lectured to international leaders at General George C. Marshall School of International Studies Program on Terrorism and Security Studies presenting on methodologies for crisis planning and preparedness. He continues to lecture nationally and internationally on crisis management, business continuity, emergency management, policy strategy, planning and preparedness, WMD, terrorism and emergency medical topics. He has published articles on related subjects and still actively participates on a number of national terrorism, all hazards preparedness and health related committees.

Mr. Gabriel is credentialed, through the International Association of Emergency Managers (IAEM) as a Certified Emergency Manager (CEM), the Disaster Recovery Institute International (DRII) as a Certified Business Continuity Professional (CBCP) and by the State of New York as a Paramedic (AEMT-P). He holds a Bachelor’s Degree (BA) from the College of New Rochelle and a Master of Public Administration Degree (MPA) from Rutgers University.
Elisabeth M. George, MS
Vice President of Global Regulation & Standards
Philips Healthcare

Elisabeth has a BS in Biomedical Engineering from Boston University and MS in Engineering Management from Northeastern University. She has working in Medical Device Regulatory for 25+ years. Her carrier began as a design engineer in Control Systems Engineering for Power Plants and then a number of years working in design, quality and test engineering for military electronics before moving into Medical Devices. Today, Elisabeth works for Philips managing and supporting the strategic planning & technical aspects quality, regulatory, security & sustainability compliance for more than 30 design & manufacturing facilities around the world. She is responsible for technical teams ensuring compliance & improvement in regulations, standards and guidance documents use in supporting product submissions, post market surveillance, product reliability, quality systems (ISO13485, 21CFR), environmental management system (ISO14001 & OHSAS 18001), software requirements & business systems. Philips product portfolio includes: X-Ray Systems, MRI Systems, CT Systems, Nuc Med Solutions and Generators, Tubes and Components. Home & Patient Solutions and supporting Information Systems along with their associated supplies and services. Her team is responsible for ISO 14971 Risk Management Program. She has participated in multiple FDA Advisory Panels as the Manufacturer’s Representative (including OB/GYN and Radiological Devices). She actively participates in industry groups and standards organizations domestically and internationally including: ANSI, AAMI, NEMA, MITA, Eucomed, COCIR and Advamed. In the past, she represented Industry and held the secretariat role for GHTF SG 4 on QMS Audit. She represented MITA on the FDA MDUFA Negotiation Team 2011/12. She actively represents Philips and Industry as a whole in technical activities like US Access Board Advisory Committee in 2012-2013 on Imaging Systems and on the 2013 FDASIA 618 HIT Policy Working Group.

Julian M. Goldman, MD
Medical Director of Biomedical Engineering
Partners HealthCare
Practicing anesthesiologist at the Massachusetts General Hospital
jmgoldman@mgh.harvard.edu

Julian M. Goldman, MD is Medical Director of Biomedical Engineering for
Partners HealthCare, and a practicing anesthesiologist at the Massachusetts
General Hospital. Dr. Goldman is the Director/PI of the Program on Medical
Device Interoperability (MD PnP) - a multi-institutional federally funded
program founded in 2004 to advance medical device interoperability to
improve patient safety and HIT innovation.

Dr. Goldman completed his anesthesiology residency and medical device
informatics fellowship at the University of Colorado, and served as a Visiting
Scholar in the FDA Medical Device Fellowship Program as well as an executive
of a medical device company. At MGH, he served as a principal
anesthesiologist in the “OR of the Future”. Dr. Goldman chairs the
international standardization committee for the safety and performance of anesthesia and respiratory
equipment (ISO TC 121) and ASTM Committee F29, Co-Chaired the HHS HIT Policy Committee FDASIA
Regulations Subcommittee and the FCC mHealth Task Force, and serves in leadership positions of AAMI,
UL, and IEC standardization committees. His awards include the AAMI Foundation/Institute for
Technology in Health Care Clinical Application Award, the International Council on Systems Engineering
Pioneer Award, and the American College of Clinical Engineering award for Professional Achievement in
Technology. E-card: www.jgoldman.info
Jeff Goldthorp is the Associate Bureau Chief for Cybersecurity and Communications Reliability of the Federal Communications Commission’s Public Safety and Homeland Security Bureau, and serves as the Acting Chief of the Cybersecurity and Communications Reliability Division. He has a leadership role in the Commission’s creative and new effort to engage communications providers in the development of a market-driven cybersecurity risk management approach, which relies on voluntary measures and assurances from communications providers as a substitute for traditional regulation. He serves as the Designated Federal Officer of the Communications Security, Reliability, and Interoperability Council (CSRIC), a federal advisory committee. CSRIC is tasked with developing voluntary mechanisms to provide macro-level assurance to the FCC and the public that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks across the enterprise. CSRIC will deliver its recommendations in March of 2015.

In May of 2012, CSRIC recommended a series of practical multi-stakeholder improvements to some of the most important cybersecurity problems facing the Internet. ISPs accounting for nearly 90% of the domestic user base have publicly announced their intention to implement these measures.

In 2009, Mr. Goldthorp led the Commission’s Cyber Security Working Group, which was tasked by the FCC Chairman with reviewing the Commission’s past cyber security work and identifying areas where the Commission may want to pursue additional steps to secure communications infrastructure. Mr. Goldthorp also made significant contributions to the Commission’s National Broadband Plan, particularly in the cybersecurity and communications infrastructure reliability and resiliency sections.

Currently, Mr. Goldthorp leads a technical and legal staff that drafts Commission and Bureau orders, Public Notices, memoranda, reports, studies and other documents relating to issues such as cybersecurity, the survivability of communications systems and networks, emergency alerting, and public safety communications. The Division also administers the Commission’s Part 4 communications disruptions reporting rules, the Network Outage Reporting System (NORS), and the Disaster Information Reporting System (DIRS). The Division analyzes data generated by these systems to spot trends and discrete problem areas in communications reliability and security.

Mr. Goldthorp earned a BSEE from Lehigh University and a MSEE from Princeton University. He is a member of Phi Beta Kappa, Tau Beta Pi, and Eta Kappa Nu.
Rick Hampton
Wireless Communications Manager
Partners Healthcare System, Boston, MA
RHAMPTON@PARTNERS.ORG

Rick Hampton is the Wireless Communications Manager for Partners Healthcare System, Boston, MA. Rick is responsible for the overall coordination of activities relating to the safe and effective use of wireless communications technologies at Partners Healthcare and its affiliates. In addition to leading internal efforts to select and design state-of-the-art systems, he coordinates efforts to provide safe and effective wireless deployments, educates Partners departments on proper wireless deployment methods and technologies, maintains and disseminates all policies regarding wireless technologies, and investigates electromagnetic compatibility and interference issues.

Since the increased use of wireless technologies brings with it increases in cybersecurity challenges, Rick also works with industry to develop responses to them.

Rick received his bachelor’s degree in Biomedical Engineering from Wright State University, Dayton, Ohio, and, for a time, attended medical school until he decided family life and engineering were much more fun. His healthcare experience includes fifteen years as a paramedic and over 25 years as a clinical engineer for three of the largest healthcare companies. His wireless background includes over 40 years working with military, commercial, amateur, and consumer wireless technologies. Rick is involved in numerous projects to raise the awareness of healthcare professionals and manufacturers regarding the safe operation and security of wireless systems of all types in healthcare facilities. Among them are the AAMI EMC Committee, AAMI Wireless Strategy Task Force, Mobile Healthcare Alliance efforts to develop a white paper on wireless use in hospitals and an IEEE RF Wireless Working Group developing guidance on the usage of radio-frequency wireless communication technologies for IEEE 1073 point-of-care medical devices that exchange vital signs and other medical device information using shared information technology infrastructures. Lately, he has been busy working with the IEC 80001 standards group to develop a risk-management model for connecting medical devices to general-purpose IT LANs. Leveraging this work for Partners, he is developing comprehensive risk management policies ensuring patient safety as well as cybersecurity for medical devices and other networked devices. Rick also consults with hospitals and medical device manufacturers on medical telemetry and communications technologies, and works with regulatory bodies to understand the effects of regulation in the context of the modern healthcare environment.
Kevin Hemsley, CISSP  
Project Manager  
Idaho National Laboratory  
Supporting the US Department of Homeland Security  
Industrial Control Systems Cyber Emergency Team (ICS-CERT)  
ics-cert@dhs.gov

Kevin Hemsley is a project manager at the Idaho National Laboratory supporting the US Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) which an operational division of the National Cybersecurity and Communications Integration Center (NCCIC). ICS-CERT works to reduce industrial control systems risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local and tribal governments, as well as industrial control systems owners, operators and vendors. In collaboration with the other NCCIC components the ICS-CERT responds to and analyzes control systems related incidents, conducts vulnerability and malware analysis, and shares and coordinates vulnerability information and threat analysis through products and alerts.

Kevin leads the ICS-CERT Vulnerability Handling team that works with independent security researchers and control system device vendors from around the world to identify and mitigate vulnerabilities affecting US critical infrastructure. ICS-CERT also coordinates medical devices vulnerabilities for DHS. Kevin has more than 20 years experience in cyber security ranging from network security to control system and SCADA security.
Mr. Hoyme has over 30 years experience in the design and development of safety-critical, real-time, fault-tolerant and secure systems in a variety of regulated domains, including medical systems, commercial and military avionics, industrial automation and space systems. He is a recognized expert in the field of systems engineering.

Mr. Hoyme is the co-chair of the AAMI Device Security working group, which is developing guidance for the application of medical safety risk standard ISO 14971 to security risk management and serves on AAMI’s Systems Engineering Advisory Board.

At Adventium Labs, Mr. Hoyme’s research focus is on safety and security-critical architectures and risk management methods for cyberphysical systems in a variety of domains, including medical devices.

Prior to joining Adventium Labs, Mr. Hoyme was a Senior Fellow at Boston Scientific where he was the systems lead for the development of the LATITUDE Remote Patient Management system. He was also the technical focal for developing standards for interconnecting implantable cardiac device data to electronic medical records systems.

Prior to joining Boston Scientific, Ken spent 18 years at Honeywell’s Corporate Research lab, where he was a Senior Fellow in their real-time computer systems group. He was awarded the H.W. Sweatt Award, Honeywell’s highest technical recognition for his work on the Boeing 777.

Ken has been granted 27 US patents. He is a member of IEEE and INCOSE. He received the Bachelors and Masters Degrees in Electrical Engineering from the University of Minnesota.
Lee Kim, JD, FHIMSS
Director of Privacy and Security
Healthcare Information and Management Systems Society (HIMSS)
lkim@himss.org

Lee Kim is the Director of Privacy and Security at the Healthcare Information and Management Systems Society (HIMSS) and a Fellow of HIMSS. HIMSS is a global, cause-based, not-for-profit organization focused on better health through information technology (IT). HIMSS leads efforts to optimize health engagements and care outcomes using information technology. Ms. Kim is a member of the SANS Institute Securing the Human Healthcare Advisory Board. Ms. Kim also serves as a Vice Chair of the American Bar Association (ABA) Health Law Section eHealth Privacy and Security Interest Group and Emerging Issues in Healthcare Law, and ABA Health eSource Editorial Board. Ms. Kim also serves as a member of the Student Leadership Award Committee for the Pittsburgh Intellectual Property Law Association. Ms. Kim is a licensed attorney in the District of Columbia and Pennsylvania and is admitted to practice before the Federal Circuit and the United States Patent and Trademark Office as a registered patent attorney. Ms. Kim holds an AV Preeminent® peer review rating in health care and intellectual property from Martindale-Hubbell. Ms. Kim is a graduate of the FBI Citizens Academy. Previously, Ms. Kim worked as a technologist in the healthcare and information technology industries and as a healthcare and intellectual property attorney in private practice.
Deborah Kobza, CGEIT, JIEM
Executive Director/CEO
National Health Information Sharing & Analysis Center (NH-ISAC)
Security Intelligence, Information Sharing & Response

NH-ISAC is the nationally recognized ISAC for the nation’s health sector by HHS, DHS, and the National Council of ISACs (representing all national critical infrastructure sector ISACs). NH-ISAC’s mission is to enable and ensure the public trust by advancing health sector cybersecurity protection and the ability to prepare for and respond to threats and vulnerabilities.

Mrs. Kobza’s 25+ years of experience and expertise includes facilitation of public/private partnerships, applied research/adoptions of leading practice principles and practices, cyber intelligence information sharing and coordinated response...all supporting national critical infrastructure resilience.

- Strategic alignment of business and technology domains (business process improvement, technology enablement, cybersecurity, business continuity and disaster recovery, regulatory compliance and enterprise IT government.
- Quality Assurance / Computer Systems Validation (IV&V) - Pharma/Medical Devices
- Security Workforce Education - Supporting DHS in the development of the IT Security Essential Body of Knowledge (EBK) and led development of a "National State Government IT Security Education Framework"; followed by supporting development and adoption of the NIST National Initiative for Cybersecurity Education (NICE) "National Cybersecurity Education Framework"
- Security Leading Practice - Supporting development and adoption of the NIST "Framework for Improving Critical Infrastructure Cybersecurity".
- State/National Security Leadership - Fostering and enabling cybersecurity economic development, research, workforce development public/private partnerships

Deborah serves as a member of the Critical Infrastructure Partnership Advisory Council (CIPAC), US DHS Cyber Unified Coordination Group (UCG), National Council of ISACs, HHS Sector Coordinating Council (SCC), SCC Cybersecurity Legislation Committee Chair, Regional Consortium Coordinating Council (RC3) and the National Critical Infrastructure Protection Plan (NIPP) Working Group.

NH-ISAC - Global Situational Awareness Center, NASA/Kennedy Space Center, FL.
Ms. Ramya Krishnan is currently a senior project engineer with the Health Devices Group at ECRI Institute. Her primary responsibilities include evaluating and testing medical devices, investigating device issues and providing consultation to ECRI hospital members on selection, purchase and appropriate use of medical equipment. More recently, Ms. Krishnan, in collaboration with ECRI Institute’s patient safety organization, has been analyzing the efficiency of Health-IT event reporting. Her areas of expertise include medical device integration with EMRs, cybersecurity of medical devices and alarm notification/ integration systems. Since joining ECRI Institute, Ms. Krishnan has evaluated several monitoring systems and has authored multiple guidance articles on cybersecurity, medical device connectivity and EMR integration for the Health Devices journal. Before joining ECRI Institute in 2008, Ms. Krishnan completed her Masters in Biomedical Engineering from Drexel University.
Darren Lacey, JD
Chief Information Security Officer and Director of IT Compliance
Johns Hopkins University and Johns Hopkins Medicine

Darren Lacey has been serving as Chief Information Security Officer and Director of IT Compliance for Johns Hopkins University and Johns Hopkins Medicine for the past ten years. He has been working in the technology sector, as a developer, attorney, consultant and executive for twenty years. He serves on several committees related to homeland security, privacy and cyber-security. He was the first Executive Director of the Johns Hopkins University Information Security Institute, a National Security Agency Center of Academic Excellence in Information Assurance.
Mary K. Logan, JD, CAE
President and CEO of the Association for the Advancement of Medical Instrumentation (AAMI)
MLogan@aami.org

Mary Logan, JD, CAE, is President and CEO of the Association for the Advancement of Medical Instrumentation (AAMI), a nonprofit membership organization whose mission is to support the health care community in the development, management and use of safe and effective medical technology. AAMI works to advance and promote the improvement of patient safety through medical technology. AAMI’s mission makes it a trusted partner of industry, healthcare institutions, subject experts, and government agencies. An American National Standards Institute (ANSI) accredited Standards Developing Organization (SDO), AAMI also provides international leadership by administering the secretariats of a number of ISO and IEC committees that develop standards.

With a law degree from the University of Wisconsin Law School, Ms. Logan is a Certified Association Executive and has over 20 years of senior management and board experience. Prior to taking the reins as President of AAMI in 2009, Ms. Logan served as Chief Operating Officer (COO) of the American Dental Association in Chicago, where in earlier years she served as its general counsel. During her tenure, the ADA was named one of the most remarkable associations in the United States in Seven Measures of Success, a report issued by the American Society of Association Executives. Ms. Logan also serves on the board of directors of the American National Standards Institute (ANSI) and is a member of its executive committee and incoming chair of its Organizational Management Forum (OMF).

Under Ms. Logan’s leadership, AAMI has grown considerably in its stature, reputation, and visibility in the healthcare community. Membership and non-dues revenue have grown in spite of a national recession, when many U.S.-based organizations have faced considerable financial strain. She has brought a new vitality to AAMI, where she and her staff have launched many new programs to serve its stakeholders. In 2013, AAMI was awarded the distinguished national GE-Pioneering Spirit Award from the American Association of Critical Care Nurses for the work of its new Healthcare Technology Safety Institute on infusion and alarm safety.

Ms. Logan lives and works in Arlington, Virginia. Her hobbies are music, walking, reading, and travel anywhere with her husband, John Stellberg. Their daughter, Sarah, started law school in the fall of 2013 at the University of Michigan.
John Lu, MBA, MS, CISSP
Principal
Deloitte & Touche LLP
jolu@deloitte.com

John is a Life Sciences Principal with over fifteen (15) years of experience in information technology, information security, data privacy, and risk management, with a focus on Medical Device Security.

- Leads the Cyber Risk Services relationship at several global Life Sciences organizations.
- Has led a variety of Medical Device Security projects at Life Sciences organizations.
- Has led a variety IAM projects (e.g., assessments, strategies, implementations, managed services) at Life Sciences organizations, as well as within other industries.
- Led several global, enterprise-wide IT risk management and IAM initiatives across various organizations, with projects typically focused on cost reduction, operational efficiency, risk mitigation, and improved security and compliance.
- Experience encompasses a broad spectrum of engagement types, ranging from project management, policy development, current state assessment, strategy and roadmap development, requirements analysis and definition, vendor evaluation and selection, architecture and design, installation and configuration, testing, and knowledge transfer.
- Possesses strong technical writing, leadership, project management, and interpersonal skills.
- Holds an MBA from Columbia University and a MS in Economics from Rutgers University, as well as certifications including CISSP, CRISC, and PMP.
William H. Maisel, MD, MPH
Chief Scientist and Deputy Center Director for Science
FDA Center for Devices and Radiological Health
William.Maisel@fda.hhs.gov

William H. Maisel, MD, MPH is Chief Scientist and Deputy Center Director for Science at FDA’s Center for Devices and Radiological Health (CDRH). He is responsible for providing leadership in the development, implementation, execution, management and direction of the Center’s broad national and international biomedical science programs.

Prior to joining FDA, Dr. Maisel was Associate Professor of Medicine at Harvard Medical School with more than 15 years of clinical experience as a Board-certified cardiologist.

He is former Chair of the FDA Circulatory System Medical Device Advisory Committee and is a former member of the Center for Medicare and Medicaid Services Coverage Advisory Committee. Dr. Maisel received his undergraduate degree in biology from MIT, his medical degree from Cornell Medical College, and his Masters in Public Health from the Harvard School of Public Health. He has published more than 120 research manuscripts, book chapters, and scientific abstracts on regulatory science, device innovation, and medical device safety and effectiveness.
Jackie McCarthy, JD
Director of Wireless Internet Development at CTIA-The Wireless Association®

Jackie McCarthy is the Director of Wireless Internet Development at CTIA-The Wireless Association®. Jackie works with stakeholders across the wireless ecosystem to develop best practices and guidelines for mobile technology’s emerging uses, including mobile health, commerce, education, and logistics. In 2013, Jackie represented CTIA on the HHS/FDA/FCC FDA Safety & Improvement Act Advisory Committee to recommend a policy framework for health IT, including mobile medical apps. She also served as a mentor at the 2014 Sprint TechStars mHealth Accelerator, and as a judge at the App Developers Alliance HealthHack in 2013. She has spoken on mobile health issues before the International Pharmaceutical Privacy Consortium, and at a TEDMed “Great Challenges in Health Care” event. Previously, Jackie served as Director of State Regulatory Affairs at CTIA, engaging with public utility commissions and other state regulatory agencies, on a variety of wireless policy issues, including broadband, intercarrier compensation, and smart grid. Prior to joining CTIA, Jackie was the Director of Government Affairs at PCIA-The Wireless Infrastructure Association. Jackie earned a B.S., with High Honors from Stetson University, and a J.D. with Honors from Emory University School of Law.
Kevin McDonald, BSN, ME-PD, CISSP  
Director of Clinical Information Security  
Mayo Clinic  
McDonald.Kevin@mayo.edu

Kevin McDonald, CISSP, is the Director of Clinical Information Security at Mayo Clinic. His responsibilities include the security of medical devices, environmental systems and clinical support systems across the Mayo Clinic sites. Kevin has over 35 years of healthcare experience in multiple roles. His healthcare experience includes critical care and emergency nursing, nursing management, electronic medical record implementation, information technology and information security. He received his undergraduate degree in Nursing and graduate degrees in Education and Information Systems.
Michael C. McNeil is the current Global Product Security & Services Officer for Philips Healthcare. In this capacity, McNeil is responsible for leading the global product security program for the company and insuring consistent repeatable processes are deployed throughout their products and services in the Healthcare market. Prior to this assignment, McNeil was the former Global Chief Privacy & Security Officer at Medtronic responsible for the development and design of their initial product security and incident response management programs; Chief IT Security Officer at Liberty Mutual Group; Global Chief Privacy Officer at Pitney Bowes, and Vice President, Chief Privacy Officer of Data Services for Reynolds & Reynolds.

McNeil is a noted security and privacy expert, he has conducted in-house training and presentations for industry, customers and clients and has presented at several security and privacy conferences worldwide. Michael is a current Governing Body Co-Chair for the Boston and Minneapolis CISO Executive Summits presented by Evanta. Michael has held the chair position for the Medical Device Privacy Consortium (MDPC) and currently holds the chair position for the MDPC Device Security Working Group which recently published the Whitepaper entitled “Security Risk Assessment Framework for Medical Devices”. He was recently named a 2013 Top 10 Breakaway Leader of Chief Information Security Officer (CISO), and was also awarded in 2013 as the First Minneapolis CISO Visionary Award in addition to the 2011 Outstanding MBA of the Year by the National Black MBA Association.
Ron Mehring, MBA, CISSP
Senior Director - Information Security & CISO
Texas Health Resources
RonaldMehring@texashealth.org

Ron Mehring serves as the CISO - Senior Director, Information Security for Texas Health Resources, one of the largest faith-based, nonprofit health care delivery systems in the United States. The system's primary service area includes 16 counties in north-central Texas, home to more than 6.2 million people.

At Texas Health Resources, Ron leads IT GRC, security architecture, security operations, and the IT BC DR program. His current initiatives are focused on improving team performance, improving resiliency management, integrating a threat-management architecture that accounts for present and emerging threats, and maturing a technology risk management program that is aligned with the strategic goals of the organization.

Ron began his career in technology for the United States Marine Corps. After 21 years of military service, Ron retired from the Marine Corps and joined the Department of Veteran Affairs where he led Compliance Assessment teams within the newly formed Oversight & Compliance group. He also served as the Department of Veterans Affairs, Deputy Director for Network & Security Operations.

Ron holds an MBA in Risk Management from NYIT and is a Certified Information Systems Security Professional (CISSP).
Mr. Murray serves as an Expert Regulatory Review Scientist with United States Food and Drug Administration. His day to day work is focused on the interpretation and application of FDA Regulations for FDA Regulated Computer and Software Products.

In addition to his 20 years at FDA, John’s professional experience includes the United States Navy Nuclear Submarine Service, Telex Computer Products, General Dynamics Corporation, and Technology Management & Analysis.

Mr. Murray earned his Bachelor of Science in Electronics Engineering from George Mason University and his Master of Science in Computer Science from Rensselaer Polytechnic Institute.
Dale Nordenberg, MD
Executive Director, MDISS
CEO, Novasano Health and Science
dalenordenberg@novasano.com

Dr. Nordenberg is CEO of Novasano Health and Science, a company that delivers information technology services and products to accelerate innovation in healthcare and life sciences. He has extensive experience in healthcare strategy and operations, health information technology, FDA regulated industries, research network development, public-private partnership development, and emergency preparedness.

Dr. Nordenberg is co-founder and Executive Director for the Medical Device Innovation, Safety, and Security Consortium (MDISS), a public-private partnership that works with device manufacturers, healthcare systems, government agencies, and other stakeholders to improve the security and safety of medical devices and biomedical device networks. He serves on the Brookings Institute Medical Device Post Market Surveillance System Planning Board and recently coordinated a National Academy of Sciences Innovation Policy Forum briefing on medical device innovation.

Prior to Novasano, Dr. Nordenberg was a managing director in the health care practice of PricewaterhouseCoopers. From 2002 through 2007, he was the Chief Information Officer and Associate Director, National Center for Infectious Diseases and was detailed to the Office of the National Coordinator for Health Information Technology, 2004-5. He was a member of the Science and Technology Review Subcommittee of the Science Advisory Board of the FDA, 2007 and 2009. Prior to CDC, Dr. Nordenberg was a founding executive of a company that launched VeriSign affiliates in Latin America and Asia; faculty in the Emory School of Medicine where he founded and directed the Office of Medical Informatics for the Emory University Children's Center and was the physician informatics lead at Egleston Children’s Hospital.

Dr. Nordenberg is a pediatrician, medical epidemiologist, and medical informaticist. He completed a BS in Microbiology from the University of Michigan, medical degree from Northwestern University, pediatrics residency at McGill University (Montreal Children’s Hospital), and fellowship in epidemiology in the Epidemic Intelligence Services Program at the Centers for Disease Control.
Gavin O’Brien, MS
Computer Scientist
National Institute of Standards and Technology (NIST)
National Cybersecurity Center of Excellence (NCCoE)

Gavin O’Brien is a computer scientist at the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE). He launched the center’s first Health IT and, since early 2013, has been overseeing a use case for mobile device security. Gavin is currently working on a second use case in medical devices specifically for infusion pumps.

Prior to joining the center in 2012, Mr. O’Brien spent 13 years at NIST’s IT Laboratory. Mr. O’Brien received a BS in Mathematics from Bates College and a MS in computer science from the University of Tennessee.
Thad Odderstol, MS  
Industry Engagement and Resilience  
Stakeholder Engagement and Cyber Infrastructure Resilience  
Cybersecurity and Communications  
U.S. Department of Homeland Security

Mr. Odderstol is the Director for Industry Engagement and Resilience (IER) Program within the Department of Homeland Security’s Office of Cybersecurity and Communications (CS&C). IER serves as the Sector Specific Agency to the Information Technology Sector and Communications Sector and provides guidance and expertise to the Critical Infrastructure cross-sector community to address National Infrastructure Protection Plan cybersecurity requirements, as well as to advisory council support and expertise to the National Safety Information Exchange (NSIE) National Security Telecommunications Advisory Committee (NSTAC). Thad has also been instrumental in the implementation of the National Institute of Standards and Technology Cybersecurity Framework and is the Program Manager for the Critical Infrastructure Cybersecurity Community (C3) Voluntary Program.

Thad’s professional background has spanned both the public and private sector, to include managing communications critical infrastructure protection efforts for the National Communications System, and programming, interactive media development, and technical project management for the safety and security product portfolio at America Online, Corp.

Mr. Odderstol holds a B.A. from George Mason University, a M.S. in Information Systems Management from The George Washington University, and is a 2014 MBA candidate with The George Washington University School of Business.
BAKUL PATEL is Associate Director for Digital Health (acting), at the Center for Devices and Radiological Health (CDRH), at the Food and Drug Administration (FDA). Mr. Patel leads regulatory policy and scientific efforts at the Center in areas related to emerging and converging areas of medical devices, wireless and information technology. This includes responsibilities for mobile health, health information technology, cyber security, medical device interoperability, and medical device software.

Mr. Patel is the FDA liaison between the Federal Communications Commission (FCC) and the Office of the National Coordinator (ONC). Since its inception in 2013, Bakul chairs the International Medical Device Regulators Forum (IMDRF) “software as a medical device” working group, a global harmonization effort.

Before joining FDA, Mr. Patel held key leadership positions working in the telecommunications industry, semiconductor capital equipment industry, wireless industry and information technology industry. His experience includes Lean Six Sigma, creating long and short-term strategy, influencing organizational change, modernizing government systems, and delivering high technology products and services in fast-paced, technology-intensive organizations.

Mr. Patel earned an MS in Electronic Systems Engineering from the University of Regina, Canada, and an MBA in International Business from The Johns Hopkins University.
Henri “Rik” Primo, MS  
Director of Strategic Relationships for the SYNGO (Imaging Informatics) Division  
Siemens Medical Solutions USA, Inc.

Henri “Rik” Primo is Director of Strategic Relationships for the SYNGO (Imaging Informatics) Division, Siemens Medical Solutions USA, Inc.

Primo’s career with Siemens began in 1998 as a Marketing Manager in the Health Services Division. His general expertise with digital imaging, PACS and healthcare information systems proved invaluable in this position.

Prior to his career in the RIS/PACS/CVIS/RIS domain, Primo managed the Biomedical Engineering and Electronic Data Processing Departments at the 500-bed Holy Family Hospital in Ghent, Belgium. Primo served as faculty member at numerous RIS/PACS events. He has been a featured speaker at the Society of Imaging Informatics in Medicine (SIIM), TEPR (USA), MSRT, CARS, RSNA, PACS 2000, AHRA, ACR, NYMIIS and other professional Societies and Organizations on the topics of digital imaging, digital imaging workflow and PACS in general. He holds patents for film digitizing technologies. He taught Digital Radiology Imaging Technologies at the University of Charleroi in Belgium from 1985 to 1988.

Primo assumed the function of Secretary and Director at the board of SIIM for six years.

He is currently the Chairman of the Medical Imaging Informatics section and member of the Board of Directors at the Medical Imaging Technology Alliance (MITA) of the National Electrical Manufacturers Association (NEMA).

He is also member of the Siemens Global Strategic Standardization Management team and provides guidance to Siemens executive management on Imaging Informatics standards, policies and technologies.

A native of Ghent, Belgium, Primo holds a degree in electrical engineering from the city’s Institute of Technology.

Since 1997 he resides in Chicago with his wife Stephanie.
Jay Radcliffe, MS, CISSP  
Senior Security Consultant and Researcher  
Rapid7  
jay_radcliffe@rapid7.com

Jay has been working in the computer security field for over twelve years, and is currently a Senior Security Consultant and Researcher for Rapid7. Coming from the managed security services industry, Jay has used just about every security device made over the last decade. Recently, Jay has presented ground breaking research on security vulnerabilities in medical devices at Black Hat and Defcon. As he is a type I diabetic, Jay has unique expertise with medical device and medical related technology. Jay holds a Masters degree in Information Security Engineering from SANS Technology Institute as well as a Bachelor’s degree in Criminal Justice/Pre-Law from Wayne State University.
Linda Ricci
Branch Chief, Cardiac Diagnostic Devices Branch
Division of Cardiovascular Devices
Office of Device Evaluation
Center for Devices and Radiological Health

Linda Ricci began her career developing artificial intelligence solutions in the defense industry. In this role she designed and developed software implementations of neural network applications. Ms. Ricci then moved to the medical device industry as a software engineer. She helped to develop several diagnostic cardiology devices and has participated in all phases of product life cycle development. Currently Ms. Ricci is the branch chief for the Cardiac Diagnostic Devices Branch in the Division of Cardiovascular Devices. In this role, she is responsible for the review of devices including automated external defibrillators, electrocardiographs, multi-parameter monitors and non-invasive blood pressure monitors. She has degrees in Electrical Engineering and Medical Engineering.
Billy Rios  
**Director of Vulnerability Research and Threat Intelligence**  
Qualys  
[mailto:billy.rios+medical@gmail.com](mailto:billy.rios+medical@gmail.com)

Billy is an accomplished author and speaker. He is currently serving as the Director of Vulnerability Research and Threat Intelligence at Qualys. Billy studies emerging threats with a focus on embedded devices, Medical Devices, Industrial Control Systems (ICS), and Critical Infrastructure (CI). Before Qualys, Billy was a Lead at Google where he led the front line response for externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft). During his time at Microsoft, Billy led the company’s response for several high profile incidents, including the response for Operation Aurora. Before Microsoft, Billy worked as a penetration tester, an intrusion detection analyst, and served as an active duty Marine Corps Officer.

Billy currently holds an MBA and a Master of Science in Information Systems. He was a contributing author for several publications including: Hacking, the Next Generation (O’Reilly), Inside Cyber Warfare (O’Reilly), and The Virtual Battle Field (IOS Press). Billy has also presented at such prestigious security conferences as Black Hat, RSA, NATO CCDCOE, Microsoft's Blue Hat, DEFCON, ToorCon Seattle, and HITB Security conference.
Suzanne B. Schwartz, MD, MBA
Director
Emergency Preparedness/Operations and Medical Countermeasures (EMCM)
Center for Devices and Radiological Health
U.S. Food and Drug Administration
Suzanne.Schwartz@fda.hhs.gov

Suzanne B. Schwartz, MD, MBA is the Director of Emergency Preparedness/Operations and Medical Countermeasures in the Center for Devices and Radiological Health (CDRH) at the FDA.

Suzanne represents CDRH/FDA across several inter-Agency initiatives and integrated program teams for the Public Health Emergency Medical Countermeasures Enterprise (PHEMCE) for chemical, biological, radiological and nuclear threats (CBRN), natural disasters and emerging infectious diseases.

As CDRH’s Emergency Operations Coordinator, Suzanne is directly involved in preparedness and incident response to matters concerning cybersecurity of medical devices and their networked systems. Her programmatic efforts in this area have evolved beyond response to include increasing awareness, outreach, partnering and coalition-building within the Healthcare and Public Health Sector. Over 2013-2014, Suzanne and her team actively participated in several working groups that are part of the Executive Order 13636 - Presidential Policy Directive 21 Integrated Task Force. Through this participation, she has served on the HHS-DHS exercise planning team for the cyber-physical functional exercise to test Deliverable #4 in the setting of a medical device cyberthreat scenario. Most recently, Suzanne now also serves as co-chair of the Government Coordinating Council (GCC) for the Healthcare and Public Health (HPH) Sector. Her efforts in this role are mainly focused on strategic engagement of Sector stakeholders to strengthen cybersecurity for the HPH critical infrastructure.

Before joining FDA, she served on the full time General Surgical faculty at the Weill Cornell Medical Center in New York City and was the Associate Director of its New York Firefighters Wound Healing Research Laboratory. In her current role, Suzanne continues to provide clinical subject matter expertise in burn trauma to FDA premarket review of products for burn management.

Suzanne earned an MD from the Albert Einstein College of Medicine of Yeshiva University in New York in 1988, trained clinically in General Surgery and Burn Trauma; an executive MBA from NYU Stern School of Business in 2012, and completed Cohort X of the National Preparedness Leadership Initiative – Harvard School of Public Health & Harvard Kennedy School of Government, executive education in June 2013.
Jeffrey Secunda, MS, MBA
Vice President of Technology & Regulatory Affairs
Advanced Medical Technology Association (AdvaMed)

Jeffrey Secunda is Vice President of Technology & Regulatory Affairs for the Advanced Medical Technology Association (AdvaMed) in Washington, DC. AdvaMed advocates for manufacturers of medical devices, diagnostic products, and medical information systems. Secunda is responsible for UDI, Postmarket Policy, and Medical Device Software issues. Secunda was Vice President of R&D for a medical sensor firm in Texas from 1996 to 2003. Secunda has more than 20 years' experience in clinical and biomedical engineering, including Massachusetts General Hospital and Children's Hospital in Boston where he founded and directed the Department of Biomedical Engineering from 1982 to 1995. Secunda was an Adjunct Assistant Professor of Biomedical Engineering at the Boston University School of Engineering.
Tim Skutt is Director, Security Portfolio at Wind River. He is focused on directing Wind River’s product capabilities for security and applying Wind River’s security products to meet customer system objectives. Tim has over 20 years of experience and extensive expertise in security and safety partitioning (MILS and ARINC 653), secure Linux, virtualization, Android, and real-time operating systems. His work experience includes 11 years at GE Aviation designing real-time, safety critical avionics and vetronics solutions, 7 years at Motorola designing cellular, radio, and multimedia communications systems, as well as work on airborne persistent surveillance systems and with the US Department of Energy Nuclear Reactor Analysis Division.
Wesley Snell Jr., CISSP
Director of the Computer Security Incident Response Center (CSIRC)
U.S. Department of Health and Human Services (HHS)

Wesley Snell Jr. is the Director of the Computer Security Incident Response Center (CSIRC) for the U.S. Department of Health and Human Services (HHS). CSIRC is responsible for coordinating HHS-wide operational cyber security activities and partnering with HHS Operating Divisions to protect IT resources from ongoing cyber-attacks.

Mr. Snell has more than 10 years of combined information security experience in areas of risk management, security architecture, and systems engineering. Prior to joining HHS, he served in strategic cyber security leadership roles in multiple private sector organizations. Wesley is a Certified Information Systems Security Professional (CISSP) and has a B.S. from Southern Polytechnic State University and a Master of Divinity from the Interdenominational Theological Center in Atlanta, GA.
Kevin Stine
Manager of the Security Outreach and Integration Group
NIST's Computer Security Division
kevin.stine@nist.gov

Kevin Stine is the Manager of the Security Outreach and Integration Group in NIST’s Computer Security Division. The group focuses on the mission-specific application of security standards, guidelines, and technologies to help organizations manage cybersecurity risk. Kevin also recently co-led development of the Framework for Reducing Cyber Risk to Critical Infrastructure which was developed in response to Executive Order 13636.
Raymond P. Strucker  
Senior Special Agent /Operations Manager  
Office of Criminal Investigations (FDA/OCI) 
U.S. Food & Drug Administration’s

Raymond P. Strucker is a Senior Special Agent /Operations Manager with the U.S. Food & Drug Administration’s Office of Criminal Investigations (FDA/OCI). Agent Strucker has over twenty four years of experience in conducting criminal investigations. He is presently assigned to the FDA/OCI’s Headquarters Office located in Rockville, Maryland where he analyzes alleged criminal activity involving FDA- regulated consumer products. His areas of expertise involve medical devices and biologic products regulated in the FDA’s Center for Devices and Radiological Health (CDRH) and Center for Biologics Evaluation and Research (CBER). In addition to his in-depth knowledge of the Food, Drug & Cosmetic Act (FDCA) and other associated criminal statutes that involve health care fraud, alleged device tampering, unapproved and misbranded products and other crimes, he has over twenty years of experience in the field of computer and digital forensics. He has initiated and assisted many federal, state and local law enforcement agencies in the investigation of a wide variety of electronic crimes and has successfully examined computer systems and peripheral storage devices for evidence related to a multitude of criminal offenses.
Commander Nikhil Thakur  
Engineer Officer in the United States Public Health Service  
Regulatory Policy Advisor for the Emergency Preparedness, Operations and Medical Countermeasures (EMCM) Program  
Office of the Center Director  
Center for Devices and Radiological Health (CDRH)

Commander Nikhil Thakur is an Engineer Officer in the United States Public Health Service. At his current duty station at the FDA, he is the Regulatory Policy Advisor for the Emergency Preparedness, Operations and Medical Countermeasures (EMCM) Program, within the Center for Devices and Radiological Health (CDRH), Office of the Center Director. He works with Subject Matter Experts within FDA, and with external Federal, Public and Private Sector partners on policy issues that impact the regulation of and guidance concerning the Public Health Emergency Preparedness and the Medical Countermeasure workspaces. He works closely with the Program Director to ensure policy decisions are appropriately grounded in the statutes and regulations that identify CDRH’s jurisdictional boundaries. When necessary, he works closely with Center Leadership to develop the appropriate medical device regulatory policy frameworks to enable CDRH to contribute to the overall mitigation of physical and cyber threats. Prior to joining the EMCM Program, he has had a combined 10 years of premarket and post-market experience within the Center for Drug Evaluation and Research (CDER) and CDRH. During this period, he had excelled in his roles as a compliance officer, reviewer, Team Leader and Mentor. CDR Thakur has significant experience working with pre and post market issues that impact drugs, devices, biologics and combination products, and has worked on several high profile post-market regulatory actions and premarket reviews for drugs and medical devices. CDR Thakur has a B.S. in Chemical Engineering from Rutgers University, and comes to the FDA from the Pharmaceutical Industry, where he focused on pharmaceutical process design, scale-up and validation.
Brigadier General (retired) Gregory J. Touhill is the Deputy Assistant Secretary for Cybersecurity Operations and Programs in the Office of Cybersecurity and Communications (CS&C) within the Department of Homeland Security (DHS), where he focuses on the development and implementation of operational programs designed to protect our government networks and critical infrastructure systems.

General Touhill retired from the U.S. Air Force in July 2013 after a distinguished career culminating as the Chief Information Officer and Director of Command, Control, Communications, and Cyber Systems at U.S. Transportation Command—one of the nation’s 10 combatant commands. A highly decorated combat leader, he served as the United States Defense Attaché to Kuwait and as the 81st Training Wing commander, where he established the Air Force’s Cyberspace Operations training programs and led the $1 billion rebuilding of Keesler AFB, Miss., in the aftermath of Hurricane Katrina.

General Touhill is a distinguished graduate of the Squadron Officer School, Air Command and Staff College, and the Advanced Communications Officer Training school, where he received the Webb Award as the top graduate. He also is a graduate of the Air War College, the Armed Forces Staff College, the Harvard University John F. Kennedy School of Government Senior Executive Fellows program, and the University of North Carolina’s Logistics and Technology Program for Executives.

General Touhill maintains the Certified Information Systems Security Professional (CISSP), Certified Acquisition Professional, and the Advanced Professional Director certifications.
Axel Wirth, MSc, CPHIMS, CISSP, HCISPP
National Healthcare Solutions Architect
Symantec Corporation
axel_wirth@symantec.com

As Solutions Architect, Axel Wirth provides strategic vision and technical leadership within Symantec’s Healthcare Vertical, serving in a consultative role to healthcare providers, industry partners, and health technology professionals.

Drawing from over 25 years of international experience in the industry, Mr. Wirth is supporting Symantec’s healthcare customers to solve their critical security and privacy, compliance, IT and datacenter management challenges. He is an active participant in industry organizations and a frequent speaker at conferences, forums, and webcasts on subjects such as cybersecurity, medical device security, mobile health infrastructure, compliance automation, IT infrastructure optimization, and other healthcare-specific topics.

His extensive background in the healthcare IT and medical imaging industries includes engineering leadership as well as strategic business development and marketing roles with Siemens Medical, Analogic Corp., Mitra Inc., Agfa Healthcare, and currently Symantec Corp. His education includes a BS Engineering degree (EE) from Fachhochschule Düsseldorf and an MS Engineering Management degree (MSEM) from The Gordon Institute of Tufts University.
Chantal Worzala, PhD
Director of Policy
American Hospital Association

Chantal Worzala, PhD, is director of policy at the American Hospital Association. Her primary area of focus is health information technology (IT) use and policy development. Dr. Worzala serves as the association’s liaison to the federal government and other organizations on health IT. Chantal has more than 15 years of experience in international and domestic health policy and has focused primarily on policies surrounding health IT and related technologies in recent years. Dr. Worzala has also led a private consulting practice and served as Senior Policy Advisor at Health Policy R&D, where she assisted a range of clients, including providers, patient advocates, and technology companies, in understanding and developing strategies to respond to ARRA, HITECH, and other health IT policies. Dr. Worzala also served as Senior Analyst for the Medicare Payment Advisory Commission. She holds a Ph.D. from the Johns Hopkins School of Public Health and an MPA from the Woodrow Wilson School at Princeton University.
Margie Zuk is a Senior Principal Cyber Security Engineer at the MITRE Corporation, with over 30 years of cyber security experience. She is currently the Cyber Engagement Lead for Healthcare in the Cyber Security Technical Center, where she leads MITRE’s support to the FDA CDRH on Medical Device Cyber Security.

As the Industry Collaboration Department Head for many years, Margie led MITRE’s work in cross sponsor initiatives and cyber partnerships providing expertise in Threat Based Defense, Cyber Threat Intelligence, Security Automation, Software Assurance, Privacy, and Social and Behavioral Science. Margie led the evolution of the cyber standards work at MITRE from the launch of CVE to the recent structured threat work with STIX and TAXII for DHS. She developed trusted partnerships with senior leaders across government and industry to establish governance models and to evolve the cyber security standards strategy. Prior to this, Margie led MITRE’s support to the National Information Assurance Partnership (NIAP). She was an initial member of the Common Evaluation Methodology Editorial Board, and participated in the development of the US scheme for the Common Criteria.

Margie has a Bachelor of Arts in Mathematics from the College of Mt. St. Vincent and a Master of Science in Computer Science from Stevens Institute of Technology.
The Food and Drug Administration (FDA) is announcing the following public workshop entitled “Collaborative Approaches for Medical Device and Healthcare Cybersecurity”. FDA, in collaboration with other stakeholders within the Department of Health and Human Services (HHS) and the Department of Homeland Security (DHS), seeks broad input from the Healthcare and Public Health (HPH) Sector on medical device and healthcare cybersecurity. The vision for this public workshop is to catalyze collaboration among all HPH stakeholders. Participants will identify barriers to promoting cooperation; discuss innovative strategies to address challenges that may jeopardize critical infrastructure; and enable proactive development of analytical tools,
processes, and best practices by the stakeholder community in order to strengthen medical device
cybersecurity.

**Dates and Times:** The public workshop will be held on October 21 and 22, 2014, from 9 a.m. to 5 p.m.

**Location:** The public workshop will be held at the National Intellectual Property Rights Coordination Center Auditorium, 2451 Crystal Dr., suite 200, Arlington, VA 22202. Entrance for the public workshop participants is through the main doors which face Crystal Drive. Upon arrival at the facility, participants should visit the registration table to check in. For parking, participants may choose from a number of pay garages, including one directly beneath the facility.

**Contact Person:** Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5418, Silver Spring, MD 20993, 301-796-6937, FAX: 301-847-8510, email: Suzanne.Schwartz@fda.hhs.gov.

**Registration:** Registration is free and available on a first-come, first-served basis. Persons interested in attending this public workshop must register online by 4 p.m., October 14, 2014. Early registration is recommended because facilities are limited and, therefore, FDA may limit the number of participants from each organization. If time and space permit, onsite registration on the day of the public workshop will be provided beginning at 8:30 a.m.

If you need special accommodations due to a disability, please contact Susan Monahan, 301-796-5661, email: Susan.Monahan@fda.hhs.gov, no later than October 15, 2014.

To register for the public workshop, please visit FDA’s Medical Devices News & Events-Workshops & Conferences calendar at [http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm](http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm). (Select
this public workshop from the posted events list.) Please provide complete contact information for each attendee, including name, title, affiliation, address, email, and telephone number. Those without Internet access should contact Suzanne Schwartz to register (see Contact Person). Registrants will receive confirmation after they have been accepted. You will be notified if you are on a waiting list.

**Streaming Webcast of the Public Workshop:** This public workshop will also be Webcast. Persons interested in viewing the Webcast must register online by 4 p.m., October 14, 2014. Early registration is recommended because Webcast connections are limited. Organizations are requested to register all participants, but to view using one connection per location. Webcast participants will be sent technical system requirements after registration and will be sent connection access information after October 16, 2014. Most updated browsers will support the Webcast.

**Comments:** FDA is holding this public workshop to obtain information on medical device cybersecurity. In order to permit the widest possible opportunity to obtain public comment, FDA is soliciting either electronic or written comments on all aspects of the public workshop topics, regardless of attendance at the public workshop. The deadline for submitting comments related to this public workshop is November 24, 2014.

Regardless of attendance at the public workshop, interested persons may submit either electronic comments regarding this document to [http://www.regulations.gov](http://www.regulations.gov) or written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. It is only necessary to send one set of comments. Identify comments with the docket number found in brackets in the heading of this document. In addition, when responding to specific questions as outlined in section III of this
document, please identify the question number you are addressing. Received comments may be seen in the Division of Dockets Management between 9 a.m. and 4 p.m., Monday through Friday, and will be posted to the docket at http://www.regulations.gov.

Transcripts: Please be advised that as soon as a transcript is available, it will be accessible at http://www.regulations.gov. It may be viewed at the Division of Dockets Management (see Comments). A transcript will also be available in either hardcopy or on CD-ROM, after submission of a Freedom of Information request. Written requests are to be sent to the Division of Freedom of Information (ELEM-1029), Food and Drug Administration, 12420 Parklawn Dr., Element Bldg., Rockville, MD 20857. A link to the transcripts will also be available approximately 45 days after the public workshop on the Internet at http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm. (Select this public workshop from the posted events list).

SUPPLEMENTARY INFORMATION:

I. Background

In February 2013, the President issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” recognizing that resilient infrastructure is essential to preserving national security, economic stability, and public health and safety in the United States (Ref. 1). Executive Order 13636 states that cyber threats to national security are among the most serious, so stakeholders must enhance the cybersecurity and resilience of critical infrastructure. This includes the HPH Sector. Furthermore, Presidential Policy Directive (P.P.D.) 21 tasks Federal Government entities to strengthen the security and resilience of critical infrastructure against physical and cyber threats such that these efforts reduce vulnerabilities, minimize consequences, and identify and disrupt threats (Ref. 2). Moreover, P.P.D. 21 encourages all public and private
owners and operators to share responsibility in achieving these outcomes. By convening this public meeting, FDA and its workshop partners strive to engage all stakeholders in HPH. These stakeholders include, but are 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); patient groups; insurance providers; cybersecurity researchers; local, State, and Federal Governments; and information security firms.

Executive Order 13636 and P.P.D. 21 together serve as a call to action for promoting the cybersecurity of the Nation’s critical infrastructure. The National Institute of Standards and Technology (NIST) developed the “Framework for Improving Critical Infrastructure Cybersecurity” (“Framework”) with collective input from government agencies and the private sector to address Executive Order 13636’s call for a voluntary, risk-based approach, harnessing a set of industry standards and best practices to manage cybersecurity risks (Ref. 3). P.P.D. 21 identifies critical sectors within the United States and charges each with adapting and implementing the Framework. HHS, as lead for the HPH Sector, seeks to adapt the Framework across its workspace. Developing a common lexicon is critical to this public-private collaboration to address and manage medical device cybersecurity risks. This workshop is an integral step towards the HPH Sector’s collective understanding of the Framework and how it might be adapted to address the unique medical device cybersecurity needs and challenges within the sector.

If exploited, cyber vulnerabilities may result in medical device malfunction, disruption of healthcare services including treatment interventions, inappropriate access to patient information, or compromised electronic health record data integrity. Such outcomes could have a profound
impact on patient care and safety. As devices become more connected and interoperable, the threat potential increases. Now, rather than impacting a single device or single system, multiple devices or an entire hospital network may be compromised. Addressing medical device cybersecurity requires recognizing interoperability and interconnectivity. Therefore, enhancing security and resilience entails designing healthcare systems for seamless integration. Such integration will foster innovative and interoperable medical devices that protect and improve patient health and safety.

Advancing medical device cybersecurity measures within the HPH Sector relies upon a ‘whole of community’ approach that will require acceptance of a ‘shared ownership and shared responsibility’ model. The objectives of such a model are twofold: (1) to seek solutions that incentivize businesses to adopt best practices and industry standards to be included in product design and systems architecture, and (2) to foster stakeholder collaboration such that emerging threat and vulnerability information is readily shared. This effort requires breaking down barriers and building trust between stakeholders. Ultimately, this effort will facilitate a forum to implement HPH cyber vulnerability and threat management.

II. Topics for Discussion at the Public Workshop

The public workshop sessions will incorporate the following general themes:

- Envisioning a collaborative environment for information sharing and developing a shared risk-assessment framework using a common lexicon;
- Overcoming barriers (perceived and real) to create a community of ‘shared ownership and shared responsibility’ within the HPH Sector to increase medical device cybersecurity;
- Gaining situational awareness of the current cyber threats to the HPH Sector,
especially to medical devices;

- Identifying cybersecurity gaps and challenges, especially end-of-life support for legacy devices and interconnectivity of medical devices;

- Adapting and implementing the Framework to support management of cybersecurity risks involving medical devices;

- Developing tools and standards to build a comprehensive cybersecurity program to meet the unique needs of the sector’s critical infrastructure, including medical devices;

- Leveraging the technical subject matter expertise of the cybersecurity researcher community working with HPH stakeholders to identify, assess, and mitigate vulnerabilities; and

- Building potential solutions: Exploring collaborative models to gather diverse experts and establish medical device security benchmarks which are continuously validated.

III. Questions for Consideration

FDA also requests HPH Sector stakeholders to provide perspective on the following:

8. Are stakeholders aware of the “Framework for Improving Critical Infrastructure Cybersecurity”? If so, how might we adapt/translate the Framework to meet the medical device cybersecurity needs of the HPH Sector?

9. How can we establish partnerships within the HPH Sector to quickly identify, analyze, communicate, and mitigate cyber threats and medical device security vulnerabilities?
10. How might the stakeholder community create incentives to encourage sharing information about medical device cyber threats and vulnerabilities?

11. What lessons learned, case studies, and best practices (from within and external to the sector) might incentivize innovation in medical device cybersecurity for the HPH Sector? What are the cybersecurity gaps from each stakeholder’s perspective: knowledge, leadership, process, technology, risk management, or others? and,

12. How do HPH stakeholders strike the balance between the need to share health information and the need to restrict access to it?

The deadline for submitting answers to these questions for consideration and any other additional comments on the proposed workshop topics is October 7, 2014.

IV. References


Dated: September 17, 2014.

Leslie Kux,

Assistant Commissioner for Policy.

[FR Doc. 2014-22515 Filed 9-22-14; 8:45 am]

BILLING CODE 4164-01-P
Notes Section: