



Workshop on Information Sharing & Safeguarding Standards Hosted by the Standards Coordinating Council (SCC)

Thursday, March 26, 2015
Hyatt Regency Hotel, 1800 Presidents Street, Reston, Virginia

AGENDA

7:30 – 9:30 AM	REGISTRATION
8.30 – 8:40 AM	Welcome & Introductions Richard Soley , Chairman & CEO, Object Management Group (OMG®)
8.40 – 9:15 AM	Opening Keynote Michael Daniels , Special Assistant to the President and Cybersecurity Coordinator
9:15 – 9:30 AM	Executive Order on Promoting Private Sector Cybersecurity Information Sharing: Tiger Team Report – The Standards Coordinating Council (SCC) Tiger Team was formed shortly after the Executive Order (EO) on Promoting Private Sector Cybersecurity Information Sharing was announced. The Team’s goal was to inventory existing assets that could support the E.O., determine SCC response, and associated actions, plus examine the possibility of including it on the SCC Pipeline. This session will provide a summary of the Team’s findings to date. MODERATOR: Jamie Clark , General Counsel, Organization for the Advancement of Structured Information Standards (OASIS) Mark Reichardt , President & Chief Executive Officer, Open Geospatial Consortium (OGC) Victor Harrison , Senior. Vice President, OMG
9:30 – 10:30 AM	Grand Ballroom ABC, 2nd Floor Opening Panel: Operationalize Project Interoperability – The panelist will discuss the goals of Project Interoperability to help government and non-government organizations identify a baseline of terms, tools and techniques to create a safe information sharing network for any type of information sharing. We are trying to normalize the way information sharing interoperability tools are developed, improved and adopted. MODERATOR: Kshemendra Paul , Program Manager, Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence (ODNI) Steve Ambrosini , Executive Director, IJIS Institute Mark Reichardt , President & Chief Executive Officer, OGC Victor Harrison , Senior. Vice President, OMG Jamie Clark , General Counsel, OASIS
10:30 – 10:50 AM	BREAK

10:50 – 11:50 AM	<p>Grand Ballroom ABC, 2nd Floor</p> <p>Mid-Morning Panel: Advances in Maritime Security Information Sharing – Significant advances in maritime security information sharing are underway at the Department of Homeland Security (DHS) thanks to the vision of the PM-ISE under Project Interoperability. By combining the proven National Information Exchange Model (NIEM), the innovative drive of the Science and Technology (S&T) Directorate and the essential, mission requirements of the U.S. Coast Guard, DHS is poised to begin implementation of a ground breaking solution for the integration and collection of maritime sensor data. By linking the Maritime ISE to the Integrated Maritime Domain Enterprise, Coastal Surveillance System, DHS is establishing a new architecture that will provide a foundation for meeting joint, enterprise requirements for information sharing capabilities at DHS, and deliver mission critical information for situational awareness, intelligence, and incident command operations. Join us to learn more about these exciting new solutions for maritime security information sharing.</p> <p>MODERATOR: Michael Brody, Director, Policy, Architecture, and Governance, Department of Homeland Security (DHS)</p> <p>MK Tribbie, Maritime Security Program Manager, Borders and Maritime Security Division, Science & Technology Directorate, DHS</p> <p>LCDR Sean Plankey, CG-261 Intelligence Cloud C4ISR, U.S. Coast Guard</p> <p>Derek Nisco, Lead Business Architect, National Information Exchange Model (NIEM) PMO, DHS</p>
11:50 AM – 12:50 PM	<p>LUNCH ON YOUR OWN</p>
12:50 – 12:55 PM	<p>Grand Ballroom ABC, 2nd Floor</p> <p>Afternoon Welcome</p> <p>Michael Howell, Deputy Program Manager, Information Sharing Environment, Office of the Director of National Intelligence (ODNI)</p>
12:55 – 1:30 PM	<p>Afternoon Plenary: Machine Readable Trustmarks – A Scalable Trust Framework for the ISE – Federated identity and access management is a key enabler for sharing of information across organizational boundaries and movement to cloud hosted services. The separation of responsibilities for vetting, credentialing, and authenticating users from responsibilities for establishing and enforcing access to resources across organizational boundaries has increased the proliferation of federations, information sharing environments, networks, and other forms of multi-party trust frameworks. These trust frameworks tend to be focused on a single community of interest or use-case and have their own set of rules and agreements which all parties must subscribe to in order to participate. Under a NIST cooperative agreement, the Georgia Tech Research Institute (GTRI) has developed a machine-readable Trustmark framework that is being piloted in the National Identity Exchange Federation (NIEF). This framework provides an innovative approach to scaling security, privacy, trust, and interoperability across existing trust framework silos and is promising core component of the future ISE.</p> <p>John Wandelt, Fellow and Division Chief, Information Exchange and Architecture Division, Georgia Tech Research Institute (GTRI)</p>
1:30 – 2:30 PM	<p>Grand Ballroom A, 2nd Floor</p> <p>Round Table Discussion: Growing the Pipeline – This session will open with an overview of, and update on the Project Interoperability Pipeline. We will then discuss the Life Cycle Maturity Model of the Common Profile and the associated strategies and requirements for the growth of the Pipeline. An interactive discussion will follow eliciting the audiences’ ideas for future Projector Interoperability Initiatives.</p> <p>Moderator: Ashwini Jarral, Director of Operations, IJIS Institute</p> <p>Maria Cardiellos, Senior Program Manager, IJIS Institute</p> <p>Denis A. Gusty, PMP, Program Manager, Homeland Security and First Responders Group, Science & Technology Directorate, DHS</p>
2:30 – 3:00 PM	<p>BREAK</p>



3:00 – 4:00 PM	<p>Grand Ballroom B, 2nd Floor</p> <p>Round Table Discussion: Leveraging Geospatial Standards – The ability to share and integrate geospatial or location information for improved situational awareness and decision making is significantly enhanced through the use of open geospatial standards, which have been adopted by industry worldwide. This roundtable discussion will highlight the benefits of geospatial standards as applied, with emphasis on applications in LE and PS. Speakers will provide examples of geospatial standards in action, and will underscore ongoing efforts to improve the ability of NIEM to more consistently and accurately reference location and to interoperate with the vast market of geospatial technologies. GeoCyber is also discussed as a major standards theme – helping to integrate the context of location and time in addressing cyber security and threats. Also discussed will be the US Geospatial Interoperability Reference Model (GIRA) – a practical guide to for executive leadership to manage program and acquisition decisions, and provide technical architecture guidance for managers and solution architects tasked to develop and implement geospatial solutions.</p> <p>Moderator: George Percivall, Chief Engineer, OGC</p> <p>Justin Stekervetz, Director, National Information Exchange Model (NIEM) Program Management Office, DHS (GEO4NIEM)</p> <p>Jamie Clark, General Counsel, OASIS (GeoCyber)</p> <p>David J. Alexander, Director, Geospatial Management Office, Office of the Chief Information Officer, DHS (GIRA)</p>
4:00 – 4:30 PM	<p>Grand Ballroom ABC, 2nd Floor</p> <p>Interactive Discussion on the Executive Order on Promoting Private Sector Cybersecurity Information Sharing: This session will seek the audiences’ ideas and input on what action the Standards Coordinating Council should take related to the E.O.</p> <p>Kshemendra Paul, PM-ISE, ODNI</p> <p>Jamie Clark, General Counsel, OASIS</p> <p>Victor Harrison, Senior. Vice President, OMG</p>
4:30 – 5:00 PM	<p>Grand Ballroom ABC, 2nd Floor</p> <p>CALL TO ACTION: Successes in 2014 and Moving Forward</p> <p>Kshemendra Paul, PM-ISE, ODNI</p>

**Thank you for attending the
2015 Workshop on Information Sharing and Safeguarding Standards**

