IN THIS ISSUE

PRESIDENT'S MESSAGE

I'm excited to share the solutions ATIS is developing to advance the ICT industry's transformation. Since our last issue of *ATIS Update*, the work continues at an accelerated pace. In this issue you will learn about our latest initiatives that are:

- Making connected vehicles more secure by bringing the automotive and ICT industries together to form a united front against cyber intrusion.

- Helping the Internet of Things — a growing area for our industry — reach its potential, not only through improved security, but also through an innovative new software library. This effort underscores our commitment to facilitating industry adoption of open source IoT solutions for smart cities, smart home, smart transport and other applications.

- Putting caller authentication standards to the test to advance industry and FCC robocalling-mitigation goals.

- Speeding the evolution to an artificial intelligence-enabled network.

- Leveraging the availability of contextual information in the IoT to support context-aware identity management.

While our accomplishments this year are many, we look ahead to 2018 and new opportunities to showcase our work at key industry events. Building on ATIS' industry knowledge leadership in GPS and timing services, we will hold our Time and Money Workshop at the New York Stock Exchange in January. In Silicon Valley in June, we hold our 27th Annual Workshop on Synchronization and Timing Systems. Also, plan now to be at the Annual Meeting of the Committees, April 30 through May 4, in Kansas City. In addition to these events, ATIS is ramping up a host of 2018 initiatives to advance our industry to a bright and exciting future. I look forward to reporting on them in the next *ATIS Update.*

Sincerely,

Susan M. Miller
President & CEO
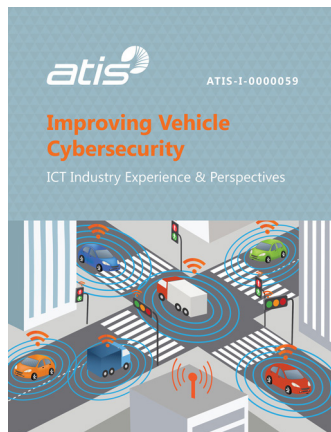
FEATURED INITIATIVES

ATIS' Board-driven Innovation Agenda is what sets many of ATIS' initiatives into motion. These priorities are addressing the ICT industry's latest imperatives and helping to advance the industry's transformation.

ADVANCING CONNECTED VEHICLE CYBERSECURITY THROUGH INDUSTRY-TO-INDUSTRY COLLABORATION

ATIS brings ICT leadership in state-of-the-art cybersecurity to vehicle original equipment manufacturers (OEMs).

Connected and self-driving vehicles bring consumers unprecedented new options, yet the risks of cyber intrusion are significant. Security breaches not only present immediate safety risks, but can also damage consumer trust in both the auto and ICT industries. Recognizing this, ATIS formed a strategic alliance with the Automotive Information Sharing and Analysis Center (Auto ISAC) to advance connected car cybersecurity.

In August, ATIS published a paper on this priority, *Improving Vehicle Cybersecurity: ICT Industry Experience & Perspectives*. It outlines the ICT industry's extensive experience in continually improving security in networks and devices, and illustrates how this can enhance security in the connected vehicle ecosystem. The network can play a valuable role in enhancing cybersecurity as it provides vehicle connectivity for advanced applications and data collection. The new report helps prepare for this by positioning both the ICT industry and vehicle OEMs to work collaboratively to secure the network and block cyber attacks or malware events — and maximize the connected vehicle's potential.

ATIS' work has received much media coverage. Our connected car cybersecurity work was covered in *Light Reading*, the AT&T blog, *Connected Car* and other outlets. In addition, the results were presented to the Auto ISAC's Community Call, a monthly update provided to all Auto ISAC members, where it generated significant interest in follow-on discussions.

ATIS INDUSTRY TESTBED ADVANCES MITIGATION OF UNWANTED ROBOCALLING AND CALLER ID SCAMS

Putting caller authentication standards to the test to ensure effectiveness.

In September, ATIS and Neustar announced that testing of caller authentication standards is well underway in a major effort to tackle the problem of unwanted calls and caller scams, with nineteen participants to date having signed on to test in the ATIS Robocalling Testbed. Through the Testbed, participants will specifically test SHAKEN implementations to ensure correct functionality, full interoperability, and operator's effectiveness in putting the SHAKEN framework into action. Testing takes place through a virtualized testbed and software implementation at a facility exclusively hosted by the Neustar Trust Lab.

By facilitating a consistent and fully interoperable implementation of SHAKEN, the testbed plays a critical role in lessening the negative impact unwanted calls have on consumers' lives – a key goal of the Federal Communications Commission's (FCC's) *Robocall Strike Force Report*. Earlier this year, the Strike Force released a report specifically highlighting the role that testing and standards have as key mitigation tools and efforts.

Anonymized and aggregated results from the Robocalling Testbed will be published by ATIS. Detailed individual results will be protected under the ATIS Testbeds Focus Group Non-Disclosure Agreement, but anonymized results can be shared, and will provide important feedback to the

industry. Further, bilateral testing outside of the ATIS Robocalling Testbed is also possible and will be included in the overall results where possible.

In other news on our work to advance robocalling mitigation, ATIS and SIP Forum Leadership met with the FTC in August to foster collaboration with the FTC regarding SHAKEN-related call display issues. As a result, the FTC provided input to the industry on the types of usability testing that may be beneficial, how the FTC can help and possible industry resources that may be able to help.

Because of its high impact, ATIS' robocalling mitigation work has received much media coverage, with one of the latest pieces coming from the *Los Angeles Times*. The September 1 article "Phone Industry Turns to James Bond for Answer to Robocall Villainy" features a picture of none other than Agent 007 himself. Visit the ATIS Press page to learn more about all the coverage this initiative is receiving.

EXPLORING THE SYNERGY BETWEEN UNMANNED AERIAL VEHICLES AND MOBILE CELLULAR SERVICES

Advancing an emerging technology with important roles in operational and infrastructure aspects of communications.

Mobile cellular networks and services are essential to advancing adoption of unmanned aerial vehicles (UAVs) or "drones." An ATIS report published in August shows the ways in which ICT boosts UAV performance, reliability and safe operation. This topic is timely as UAVs are being used for an increasing diversity of applications. These range from deliveries and flying cameras to public safety applications, agriculture, inspection of critical infrastructure including cell towers, and

more. As the number of drones in the air and their flying time increases, safety, security and privacy concerns are coming to light.

Unmanned Aerial Vehicle Utilization of Cellular Services: Enabling Scalable and Safe Operation shows how services available from mobile cellular networks address these concerns to accelerate the use of drone technology. Communication, location and identity services are highlighted. Better understanding of how UAVs and mobile cellular service technologies work together will benefit both the ICT and UAV industries. Upcoming ATIS analysis on this topic will consider payload aspects of UAV flights, including the use of UAVs to provide wireless services, for example for coverage in emergencies or during special events.

SUBSCRIPTIONLESS DEVICES AND SERVICES IN SERVICE PROVIDER NETWORKS

New models enabled by emerging 5G network capabilities.

The emergence of Internet of Things (IoT)-based services is expected to create explosive demand for new devices and applications. Although a large percentage of IoT devices will ride "over-the-top" of existing network subscriptions, many devices must still acquire network access from public (typically paid) wide area networks and, traditionally, must have a subscription with the network operator to do this. A new ATIS report explores a variety of subscriptionless device models that benefit both the user and the network operator. The report describes new models enabled by emerging 5G network capabilities that contribute to more efficient use of network resources and support new network services.

For many IoT users, the direct IoT device connectivity subscription cost structure is often higher than the willingness to pay, given the utility of the device in question. Additionally, many end users have a desire to connect to their network of choice for "occasional" data without having to maintain an ongoing subscription. The

subscriptionless device model can potentially reduce the cost and complexity for network operators as the network operator may not need to bear the full cost of maintaining "billions" of subscriptions for devices which may attach only occasionally to their network. Rather, operating models are described where the operator's primary relationship is with a third-party authentication or application service provider instead of the device itself. Some of the subscriptionless models are more naturally resistant to botnet security related attacks and can provide an extra measure of security within the IoT context. Although this paper considers the case for subscriptionless devices, this does not preclude the existence of a subscription with other third-party entities to facilitate proper charging and security for network services.

Access *Subscriptionless Devices and Services in Service Provider Networks* (ATIS I-0000061) in the ATIS White Paper Center.

SECURING CRITICAL NETWORK INFRASTRUCTURE

Addressing growing and evolving cyber threats.

In July, ATIS announced publication of two major industry resources to secure critical network infrastructure against growing and evolving cyber threats: (1) *Cybersecurity Architectural Risk Analysis Process* (ATIS-I-0000057); and (2) *Securing Internet of Things (IoT) Services Involving Network Operators* (ATIS-I-0000056).

- *Cybersecurity Architectural Risk Analysis Process* addresses proactive mitigation steps for cybersecurity attacks in addition to procedures to determine security goals and identify and assess potential risks. Industry best practices underlie many of the steps included. The document includes an example of how the Architectural Risk Analysis is used for a hypothetical health monitoring device and associated services delivered in an ICT service-provider-managed context.

- *Securing Internet of Things (IoT) Services Involving Network Operators* focuses on the security concerns associated with the rapid growth in IoT services. ATIS' work is geared toward protecting IoT services and preventing IoT equipment from becoming a source of attacks against other service users. The white paper characterizes the different levels of partnering possible between network operators and IoT service providers. Practices to proactively address the security implications in each are provided.

IoT cybersecurity, in particular, requires collaboration between devices and network providers. These two new documents help service providers adopt a more proactive approach to cybersecurity by offering a systematic process to identify and address vulnerabilities at the service design stage.

INNOVATION AGENDA PRIORITIES ON THE HORIZON

The following priorities are now on the Innovation Agenda, and launch plans are being finalized.

Evolution to an AI-Enabled Network. Artificial Intelligence (AI) is intelligence exhibited by machines or computational systems that perceive their environment and take actions that maximize the chance of success at some goal. We typically consider AI to be systems that perform some form of reasoning, planning or object management, using knowledge as well as perceived information that, in the near past, required human intervention.

For network operators, there are two classes of AI applications, those that run over the network for the benefit of an end user/client of the network and those that run within the network to optimize some aspect of network operation. End user/client applications of AI may place specific requirements on network performance and may be enhanced by specific network services. Network AI could be used to enhance network planning, NFV

orchestration, and management functions (typically operating with a long-time constant) or could be used in near real-time to dynamically optimize network performance based on rapidly changing traffic patterns. Key AI questions for network operators, to be addressed in ATIS' upcoming work in this area include:

- What classes of end user/client focused AI applications exist and what requirements does each class place on network capacity and performance? Are there specific network services that could enhance these end user AI applications?

- What specific network functions can most benefit from AI applied to network operations?

- What "near real-time" network functions (such as the Radio Access Network Self-Organizing Networks or "RAN SON" work that has been deployed in the recent past) could be enhanced with AI to provide for dynamic network optimization?

ATIS' new Ad Hoc will be considering these questions in creating an overall landscape of the AI space from a network operator perspective.

Context-Aware Identity Management. Today, there are a diversity of approaches to applying identity management (IdM) across the ICT sector and the many vertical industries that are expected to intersect with ICT in the future. In its simplest form, identity management authorizes an individual to gain access to a prescribed set of resources that are deemed allowable based on a granted set of privileges. Of course, as the demands for data and information security become more stringent, IdM has progressed and may include any combination of secure single sign-on, tokens, smart cards, multi-factor authentication, biometric authentication, etc.

If we fast forward to billions of IoT devices accessing tens of billions of applications that may be accessing data (with or without human intervention), current methods for IdM will become challenged and will likely become obsolete in the near future. At the same time, the industry has a unique opportunity to leverage new capabilities built on top of context-awareness to propel IdM to the next generation of solutions. This will require that policies be established that link context to robust identity and access management approaches. Even more important, context-aware IdM solutions that can span across industries will be far superior to a set of separate IdM approaches that are locked to specific verticals and related applications. Consumer adoption of many new IoT applications will be shaped by the ability for an individual or device to execute applications across vertical sectors without multiple IdM processes intervening across the user experience. This will be particularly important in applications that intersect between ICT and connected vehicles, eHealth, Smart Cities, Smart Home and many other sectors. ATIS' work in this area will:

- Identify the attributes of next generation context-aware networks that can contribute to the application of enhanced IdM principles (e.g., location, presence, profile, environment, situational/social awareness)

- Develop a framework view that applies contextual information to the requirements for IdM, considering future network topologies and characteristics

- Explore approaches to the application of context-aware IdM to applications that span the ICT industry and adjoining verticals. Identify the key foundational items that will enable this environment (e.g., a singular IdM policy management function)

- Summarize the key benefits to the industry and identify evolutionary path(s), understanding that network operators are well-positioned to access contextual information.

- Determine what standards or industry collaborative activities would be required to promote the concept of context-aware IdM.

A report of key context-aware IdM findings will be developed and is expected to lead to specific ATIS collaborative activities that will promote early adoption of these principles.

TECHNOLOGY AND OPERATIONS COUNCIL INITIATIVES

NEW OPEN SOURCE IOT SOFTWARE LIBRARY SIMPLIFIES CONNECTIVITY AND SECURITY FOR IOT DEVICE DEVELOPERS

Helping IoT app developers more easily connect their products to the open, interoperable oneM2M ecosystem.

In September, ATIS announced the first release of its new Open Source Internet of Things (OS-IoT) software library. The software evolved from the strong message from ATIS members that maximizing the value of common technical platforms for the industry requires not just open standards, but open source implementations of those standards, and this is even more important to IoT. The global oneM2M standard defines a common, interoperable, platform for IoT systems, providing application-independent building blocks that fulfill the core tasks of data collection, management and distribution needed by IoT solutions. oneM2M already has interworking to multiple other IoT technologies and transport technologies, and is now being used successfully in a number of industrial and consumer applications in the areas of Smart Cities, eHealth and the Smart Grid.

Until ATIS developed OS-IoT, however, no open source lightweight client platform existed to help bring the power of oneM2M to smaller scale applications. This new platform is designed to bring oneM2M benefits to a burgeoning market of developers and innovations in the areas of smart metering, smart city/transport and wearables, to name just a few. By using the OS-IoT library, instead of having to deal with networks and protocols, developers are freed to focus on the

unique, value-added aspects of their applications. OS-IoT is seen as a critical resource in helping to boost oneM2M adoption for smart devices and other smaller-scale embedded applications.

ATIS demonstrated its Open Source IoT (OS-IoT) software at ETSI IoT Week, which took place October 23-26, at the European Telecommunications Standards Institute (ETSI) in Sophia Antipolis, France. Learn more about OS-IoT at https://www.os-iot.org.

SOLUTIONS AND STANDARDS

ATIS AND MEF JOINTLY PUBLISH NEW INTERNATIONAL STANDARD FOR ORDERING CARRIER ETHERNET SERVICES

Accelerating service delivery over a more efficient ecosystem of connected networks.

In September, ATIS and MEF announced the release of a new, jointly developed specification that defines the process for ordering Carrier Ethernet services on a global basis. This standard, *Ethernet Ordering Technical Specification: Business Requirements and Use Cases*, is an important step toward creating a worldwide ecosystem of automated and interconnected networks that deliver agile, assured, and orchestrated services. This specification supports requirements defined in the *LSO (Lifecycle Service Orchestration) Reference Architecture and Framework* (MEF 55) for ordering services over the LSO Sonata interface related to inter-provider service orchestration. Information contained in the new specification will be used by both buyer and seller ordering systems for developing automated LSO API systems. This new joint specification makes the ordering process easier for customers while also advancing service provider business imperatives.

ATIS ENHANCES THE WIRELESS EMERGENCY ALERT SYSTEM

Preparing the Wireless Emergency Alerts system for the future.

ATIS is currently undertaking a major effort to update the critical standards and solutions that make the Wireless Emergency Alert (WEA) system possible. In 2011, ATIS developed the original WEA "C" interface between the government and commercial mobile service providers, which helped to set the current WEA system into action. In light of the FCC's Enhanced Wireless Emergency Alerts Report and Order (R&O), ATIS is revamping the suite of standards to prepare the WEA system for the future. Areas addressed include: increasing the maximum alert message length, no longer limiting alert texts to 90 characters; allowing the transmission of embedded URLs and phone numbers; and supporting Spanish language alerts.

This work, conducted by ATIS' Wireless Technologies and Systems Committee (WTSC), is progressing rapidly. Three major ATIS supplements were published in September, well-ahead of the November deadline:

- *ATIS Supplement B to J-STD-100, CMAS Mobile Device Behavior Specification* (ATIS-0700032), to remove the restrictions on embedded URLs and embedded telephone numbers in WEA messages as well as enhance other requirements

- *ATIS Supplement C to J-STD-101, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification* (ATIS-0700033)

- *ATIS Supplement B to J-STD-102, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification* (ATIS-0700034)

By year end, multiple new documents are targeted for publication, including the *Enhanced Wireless Emergency Alert (eWEA) Federal Alert Gateway to CMSP Gateway Interface Specification* (ATIS-0700037), an update to the original WEA standard, as well as *Cell Broadcast Entity (CBE) to Cell Broadcast Center (CBC) Interface Specification, Revision 2* (ATIS-0700008.v002).

INSIGHT INTO GPS VULNERABILITY, IMPACT ON TELECOM AND ALTERNATIVES TO GPS TIMING PROVIDED IN NEW ATIS REPORT

Better understanding how to improve the accuracy of network timing.

In September, ATIS announced the release of a major resource to help better understand and address the vulnerabilities in the Global Positioning System (GPS). Requirements for precise time delivery have driven the industry toward the increased use of GPS and GPS-dependent technologies. Yet this has left the industry vulnerable to disruptions and manipulations of the GPS signal. The new report, *GPS Vulnerability* (ATIS-0900005), provides insight into the sources of the most common problems with GPS and their impacts. It also covers several mature proposed solutions that would satisfy telecommunications sector timing requirements.

Also as part of its work to ensure the accuracy of the GPS-derived timing that networks operators depend on, in August, ATIS' Synchronization Committee (SYNC) applauded Congressional action on a backup to the existing GPS system. The National Defense Authorization Act of 2018 recognizes the need to develop an appropriate backup system for GPS that can meet industry needs for wide-area coverage, accuracy and resiliency. ATIS SYNC commended the recent $10M appropriation for the proof of concept of a GPS complementary and backup system within the House version of the Defense Appropriations Act and noted it looks forward to continued engagement with the Department of Transportation and Department of Homeland Security on these issues.

NEWS

ATIS ATTENDS TWENTY-FIRST GLOBAL STANDARDS COLLABORATION MEETING IN VIENNA

With ATIS President and CEO Susan Miller and Director, Global Standards Development Steve Barclay attending, the 21st meeting of the Global Standards Collaboration (GSC) took place from September 26-27, 2017. The event was hosted by the IEEE Standards Association (IEEE-SA) at the IEEE European office in Vienna, Austria. GSC members shared their priorities and focused on Artificial Intelligence and Smart Cities. GSC members also took the opportunity to share information on Intelligent Transportation Systems. The next GSC meeting will be held in Switzerland, hosted by IEC and ISO. For further information on GSC-21, visit gsc.ieee.org.

ATIS INSIGHTS BLOG COVERS ATIS' ROLE IN THE INDUSTRY'S HOTTEST COLLABORATIVE SOLUTIONS

Continually updated, ATIS' blog is delivering insight into some of ATIS' recent initiatives, including our work to mitigate robocalling, our GPS vulnerabilities work, our connected car initiative and our AppID Registry, which is designed to secure the IoT. Access in-depth coverage of ATIS' work on:

- Joining Forces to Make the FCC's Robocalling Initiative a Reality

- Why Time May Not Be on Your Side

- Securing the Connected Vehicle: Why a Collaborative Approach is Critical for Success

- App-ID Registry: Securing the Internet of Things (IoT)

ATIS WEIGHS IN ON THE PROMISE OF 5G

An article in the July/August issue of the Consumer Technology Association's *It Is Innovation* (*i3*) magazine entitled "The Promise of 5G" features mention of ATIS' 5G work with quotes by Senior Technology Consultant Tom Anderson. The piece also mentions our *Smart Cities Technology Roadmap* and the integration of new technologies – including 5G – as a fundamental building block for the "high bandwidth, low latency and pervasive connectivity" in smart cities.

i3 is CTA's flagship magazine focusing on innovation in technology, policy and business as well as the entrepreneurs, industry leaders and startups that grow the consumer technology industry. Access the article and see the recognition ATIS' work is receiving!

Also, ATIS was also quoted in the October 2017 feature "5G Enables Smart Cities," which was part of CTA's 5 Technology Trends to Watch series. Read to learn how fast, focused wireless technology will revolutionize our connected world – and ATIS' insight on this transformation.

FEATURED ATIS EVENTS

ATIS' TIME & MONEY II CONFERENCE ADDRESSES TIME SYNC FOR FINANCIAL MARKETS

Building on the success of the first Time and Money Conference, ATIS holds Time and Money (TAM) II, January 23, 2018, at the New York Stock Exchange. TAM II is where the experts gather to provide in-depth insight into one of the finance industry's leading concerns: the need to ensure to clients and regulators that financial transactions are accurately timed – down to the microsecond. Learn more at atis.org/tam. Register today!

PLAN NOW TO ATTEND AMOC 2018

The Annual Meeting of the Committees is the ICT industry's solutions-development focal point, where ATIS Committee and Forum participants hold meetings, conduct joint work programs, and collaborate. Join us April 30 – May 4 in Kansas City, Missouri. Register soon to secure your room at the Kansas City Marriott Downtown where AMOC Committee meetings as well as some of the event's networking events are being held. Learn more at atis.org/amoc. Register today!

PEG 2018: THE INDUSTRY'S "GO-TO" EVENT FOR PROTECTION ENGINEERING

The ATIS Protection Engineers Group (PEG) Conference will be held March 13 – 15 2018, at ADTRAN Headquarters in Huntsville, Alabama. The 2018 PEG Conference has the theme of "Improving Network Infrastructure Reliability and Sustainability," and promotes discussion on how basic electrical protection principles are applied to today's network, and the challenges of providing media services in more decentralized networks. Learn more at atis.org/peg. Register today!

WSTS 2018: NORTH AMERICA'S PREMIER TIMING AND SYNC EVENT

The 27th Annual Workshop on Synchronization and Timing Systems (WSTS), sponsored by NIST and ATIS, will take place June 18-21, 2018 in San Jose, CA. WSTS is a vendor-neutral technology workshop that addresses evolving sync requirements, as well as the roll-out of new sync systems and standards and their impact on industries and equipment manufacturers. The event builds on ATIS' positioning as an industry knowledge leader in the area of GPS and timing services. Agenda and registration information will be available shortly at atis.org/wsts.

INDUSTRY EVENTS

SIP NETWORK OPERATORS CONFERENCE

November 28 - 30, 2017
Herndon, VA
www.sipnoc.org

FIERCEWIRELESS NEXT GEN WIRELESS NETWORKS SUMMIT

November 28 - 29, 2017
Dallas, TX
www.nextgenwirelesssummit.com

SCWS AMERICAS

December 5 - 6, 2017
San Jose, CA
www.scwsamericas.com

SMART CITIES INTERNATIONAL SYMPOSIUM

January 17-18, 2018
Chicago, IL
www.smartcities-symposium.com

The Symposium brings together key thought leaders and industry practitioners to explore the most recent technology advances, business models, and lessons learned to date in making the Smart City a reality. The focus is on municipal governments and innovators who are pushing the envelope toward actual implementation of the Smart City vision. Early bird registration is available through December 15.

Must See Session:
To Open Smart City Data or Not
Thursday, January 18, 2018
10:45 am - 12:15 pm

Moderator:

- Jason Hare
  Open Data Evangelist, OpenDataSoft

Panelists:

- Paul Baker
  CEO, Webitects

- **Mike Nawrocki**
  VP of Technology and Solutions, ATIS

- David Portnoy
  Founder, Demand-Driven Open Data

Register today and receive a 15 percent ATIS member discount using the code **ATIS15**.