THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 11 NUMBER 5

NOVEMBER 2012
COMMUNICATIONS SECTOR

EDITORIAL STAFF

EDITORS
Olivia Pacheco
Kendal Smith

JMU COORDINATORS
Ben Delp
Ken Newbold

PUBLISHER
Imani Dunigan

Contact: ksmic@gmu.edu
703.993.4792

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

GEORGE MASON UNIVERSITY

School of Law

CENTER
for
INFRASTRUCTURE PROTECTION
and
HOMELAND SECURITY

This month's issue of *The CIP Report* focuses on the Communications Sector. As recent disasters such as Hurricane Sandy show, the security and resilience of our communication systems are vital to our national well-being.

In our first article, Marcus Sachs, Vice Chair of the U.S. Communications Sector Coordinating Council, provides a Sector overview. Maryland Statewide Interoperabilty Director Ray Lehr then explains the importance of communications interoperability for public safety. Next, Telecommunications Industry Association President Grant Seiffert addresses cloud infrastructure security, and Internet Security Alliance President Larry Clinton discusses the evolution of the cyber threat in the communications industry. Finally, Nadya Bartol, Senior Cybersecurity Strategist at Utilitites Telecom Council, examines the relationship between the cyber supply chain and utilities telecommunications networks.

This month's *Legal Insights* evaluates the potenial legal implications of meshnets, particularly regarding net neutrality, illegal content, and surveillance standards.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

An Overview of the U.S. Communications Sector

by Marcus H. Sachs, Vice Chair, U.S. Communications Sector Coordinating Council

The Communications Sector is an integral component of the economy – underlying the operations of all businesses, public safety organizations, and government. Communications Sector partners strive to ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored in the event of a natural disaster or man-made disruption.

The Sector has a long history of national security and emergency preparedness (NS/EP) communications cooperation among its members and with the Federal government. Symbolic of the Sector are the numerous cooperative and trusted relationships that enable the delivery of critical services when emergencies and disasters occur.

Because of the privatized nature of America's communication infrastructure, the responsibility for protecting critical networks and assets lies mostly within the private sector. Working with the Federal government, owners and operators are able to predict, anticipate, and respond to Sector outages much faster than if left on their own. Also, a strong government partnership helps industry understand how network incidents might affect the ability of the national leadership to communicate during times of crisis, how they impact the operations of other sectors, as well as the impact on response and recovery efforts.

Sector Partnerships

Partnerships between the public and private sectors represent an emerging approach to cooperative protection of critical assets that cannot be fully defended by governmental organizations alone. In the United States the private sector owns and operates nearly all of the Nation's critical infrastructure, while government agencies have access to sensitive threat information that may not be available to the private sector. Both control security programs, research and development, and other resources that may be more effective if discussed and shared in a partnership setting.

One of the most effective approaches to partnerships remains the creation of Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) by Homeland Security Presidential Directive 7 in 2005. Each of the eighteen critical infrastructure and key resource sectors have designed their coordinating councils slightly differently to best fit the organization of the sector as well as existing cultural and operational norms. The Communications Sector includes wireline, wireless, satellite, cable, and broadcasting transport networks that are all part of an even larger global communications infrastructure. The Sector integrates all five of those communications methods into one partnership with the government.

Thirty-two private sector organizations and their respective trade associations form the Communications Sector Coordinating Council (CSCC), and eleven Federal departments and their agency representatives from the Communications Government Coordinating Council (CGCC). Together with older partnerships such as the Communications Information Sharing and Analysis Center (Comm-ISAC), the Network Security Information Exchanges (NSIE), and the President's National Security Telecommunications Advisory Committee (NSTAC), the Sector exemplifies strong partnerships that provide government and industry response coordination and information-sharing mechanisms.

The Sector goals are:

- Protection and enhancement of the overall physical and logical health of communications networks

- Capability to rapidly reconstitute critical communications services in

(Continued on Page 11)

Communications: The Essential Link for Public Safety

by Ray Lehr, Maryland Statewide Interoperability Director

In today's highly technical world, with social media impacting everyone's life on sometimes a moment to moment basis, it is difficult for the public to grasp why public safety users are still struggling with interoperability. For most college students, access to their Facebook account, Twitter, and all of their friends is instantaneous; no matter what smart phone they use or in what city they are located. Unfortunately, that is not the same for public safety communications. The first responder community has been voicing the need for police, fire fighters, Emergency Medical Services, and Emergency Management to have the ability to talk to one another in times of crisis; but the challenges to make that a reality are great.

Most everyone is aware of the difficulties in communications that occurred during the attacks of September 11th. A NYPD helicopter circling above the chaos of the World Trade Center (WTC) complex sent an urgent radio transmission that the South Tower was totally engulfed and likely to collapse. Many NYPD forces heard that transmission and began to evacuate. Unfortunately, the fire forces were not on the same radio system and therefore never received a warning. That story has been used by my boss, Governor Martin O'Malley of Maryland, whenever he is asked to justify the investment of millions of dollars in infrastructure to establish a Statewide Public Safety Communications System for Maryland's first responders. The 9-11 Commission Report cited the lack of adequate communications as a root cause for some of the loss of lives during the WTC operations.

The response in our region to the Pentagon attack was much better due to the daily cooperation that the Northern Virginia public safety agencies had developed over the years. But overloading of channels and difficulty interacting with a large Federal response presented challenges at that event also. As a result, Congress took note and began to fund interoperability for public safety agencies across the country.

So what was the problem? It was multi-faceted. Over the years, the Federal Communications Commission (FCC) had assigned frequencies to public safety without a focus on interoperability. Spectrum, the radio waves, is a finite resource, and the FCC regulates not just the bands that public safety uses, but all commercial and private radio spectrum. Public safety was given frequencies in several different bands (low band, UHF, VHF, and 800 MHz) based on what frequencies were available in the region. A police or fire department operating in the UHF band cannot communicate with an agency operating in a different band. In addition, different manufactures used different technology which meant that even if you and your neighboring public safety agency were in the same band, the radio equipment made communications incompatible. Some early attempts at interoperability involved "patching" of different radio systems together. But this usually occurred on the scene when needed, and it took time to get the equipment on site and the connections made. Even then the patching reduced the quality of the transmissions, and operations were limited to just a few channels.

With the creation of DHS and specifically the Office of Emergency Communications (OEC), the United States now had a strong advocate for assisting the public safety community in finally putting the plans in place to achieve interoperability. OEC encouraged, through several grant programs, the establishment of a State plan for achieving interoperability, called a Statewide Communications Interoperability Plan . Over the next few years, States used the self assessment to channel grant dollars to projects that would allow any first responder to communicate no matter where they were deployed for an emergency. Hurricane Katrina and other disasters pointed

(Continued on Page 12)

Protecting the Communications Infrastructure

by Grant Seiffert, President, Telecommunications Industry Association

Whether on the chaotic front lines of a military engagement or in the quiet intensity of a corporate IT department, the steady, effective communication of accurate data is critical to getting the right resources to the right location at the right time. The reliable flow of data has become indispensable to modern life – whether it involves communication via radio, mobile and IP platforms, or security cameras, sensors and remote-controlled devices that need to talk to each other to complete their tasks.

With so much data being transmitted over so many devices and platforms, it becomes essential that the delivery infrastructure never fails or becomes compromised. It is for this reason that the Telecommunications Industry Association (TIA) is focused on developing standards that guarantee the survivability and security of the communications infrastructure. Through the leading trade association representing the global information and communications technology (ICT) industry, TIA member companies are involved in a range of communications sectors, including telecom, broadband, mobile wireless, information technology, networks, cable, satellite, unified communications, emergency communications, and green technology. Accordingly, it is a priority to identify coverage gaps and develop pertinent standards.

Identifying Gaps

One area currently facing security threats is cloud computing. The National Institute of Standards and Technology (NIST) identifies gaps in standards coverage for the cloud in its report, US Government Cloud Computing Technology Roadmap, Volume II - Useful Information for Cloud Adopters (Draft), published November 2011.[1]

In response to this report, TIA's Engineering Committees are working on standards to close these security gaps. Of particular, current interest is the infrastructure security for the cloud and for the infrastructure that connects people and devices to the cloud.

Cloud Infrastructure

While the security of "the cloud" has been the subject of many white papers, business reports and advertising programs, the NIST report identifies "Physical Security" as the fourth specific topic identified in Table 3 of Clause 3.1.3.3, *Cross-cutting Security System Requirements*. The report states: "FISMA security standards not only apply to security protocols implementable using hardware or software, but also to the physical security of the facilities used to house the equipment and services. Physical security includes all measures whose purpose is to prevent physical access to a building, resource, or stored information. These physical security requirements apply to third parties engaged by cloud brokers."[2]

The goal of TIA's TR-42 Engineering Committee on *Telecommunications Cabling Systems*, is to develop voluntary telecommunications standards for telecommunications cabling infrastructure in user-owned buildings, such as commercial buildings and data centers among others. In February of 2012, the TR-42 Engineering Committee created a Task Group on Network Security to identify and develop appropriate content to address this cloud security gap identified in the NIST report.

This TIA Task Group on Network Security is comprised of experts in data centers, cabling, administration systems, and physical infrastructure. Since February, the Task Group has been collecting information and

(Continued on Page 5)

[1] Available **here.**

[2] Ibid., at 37.

Cloud Infrastructure *(Cont. from 4)*

contributions on various security aspects of the (passive) physical plant, including cable security, telecommunications spaces security, wireless access point security, and pathway security. Using this information, the Task Group is developing standards to combat four threats: intrusion, sabotage, vandalism, and theft.

The Task Group noted that the ANSI/TIA-942 Standard, *Telecommunications Infrastructure Standard for Data Centers* (published by the TR42.1 Engineering Subcommittee) already provides requirements and guidelines for several security-related subjects involving data centers, which serve as the engines of the cloud. This document includes security-related requirements and guidelines appropriate for data centers on the placement of telecommunications spaces, architectural considerations, signage, cable routing, access points, supporting equipment and site selection.

Security of Cloud Access

While the NIST report focuses on data centers as a specific type of premises, prudence would dictate that similar guidance apply to the physical security for other types of premises where cloud access is of particular importance. These other premises include health care facilities, educational facilities, airports, hotels, government offices, courts, prisons, commercial buildings, industrial facilities, etc. The NIST report establishes this in Clause 5, *High-Priority Security Requirements*, which ensure that: "Well-defined resource abstraction layers (infrastructure, platform, and software apps) bring more architectural flexibility, allowing for application of more effective security countermeasures at each layer, resulting in better 'defense in depth' compared with traditional, rigid security controls relying on physical attributes (such as specific devices, MAC addresses, etc.)."[3]

Accordingly, the TIA Task Group on Network Security is not limiting the focus of the discussions to data centers. That is because the ability to connect to and access these data centers is equally important to maintaining the security of the data center itself.

The Task Group on Network Security has reported that installation guidelines applying to other types of premises are covered in existing TIA standards, including ANSI/TIA-569, *Telecommunications Pathways* and Spaces; ANSI/TIA-568-C.0, *Generic Telecommunications Cabling for Customer Premises*; ANSI/TIA-568-C.1, *Commercial Building Telecommunications Cabling Standard*; ANSI/TIA-606, *Administration Standard for Telecommunications Infrastructure*; and others.

Visibility and Control

The TIA Task Group has also noted another section of Clause 5 in the report, which states: "The (perceived) lack of visibility and control over the IT assets often runs counter to the existing security policies and practices that assume complete organizational ownership and physical security boundaries…."[4] Accordingly, in discussions about intrusion, our Task Group has been discussing important aspects of physical security, including the recognition of unauthorized modifications or re-routing of a network path. The Task Group has developed recommendations related to how the telecommunications infrastructure design should be a component of the facility's security plan.

Additionally, the TIA Network Security Task Group is developing guidelines for automated systems that should enhance the security of the cabling. The automated functions might include such features as detecting changes to patch cord placement, connection to inactive or open equipment ports, and interruption in signal traffic. These draft guidelines recommend incorporating appropriate actions in response to any alarm condition. These actions might include activating external device alarms and security video devices that feed detailed and useful information to appropriate personnel and systems. While these types of systems are already available in the market, the need for some minimum level of consistency in the services provided is essential

(Continued on Page 13)

[3] Ibid., at 49.

[4] Ibid.

The Evolution of the Cyber Threat and Cybersecurity Policy

by Larry Clinton, President and CEO, Internet Security Alliance

The year 2010 consisted of 525,600 minutes and, on average, during every one of these minutes 50 new malicious web sites were launched, 450 new versions of malicious malware were developed, 400 thousand identities were stolen, and 2 million dollars worth of intellectual property were stolen in cyber space.

As we reach the end of 2012 things have gotten much worse.

While we are still seeing virtually constant forms of traditional attacks ranging from Distributed Denial of Service, (DOSS) to Botnet to Phishing attacks, we have also seen an evolution in the paradigm of cyber attacks.

The so called Advanced Persistent Threat, (APT) which was, until recently, largely confined to government and military targets, has evolved and defused throughout our critical infrastructure. These ultra sophisticated attackers, once confined to nation states attacking nation states, are now using advanced techniques against all forms of critical infrastructure including the electric grid and our telecommunications networks.

Telecommunications providers have been aggressive in launching a wide variety of programs to address the cyber threat, often at shareholder expense. Among the most notable of these are the Verizon/ Secrete Service[1] work to identify successful best practices that can prevent or mitigate the effects of most traditional attacks, Comcast's "Constant Guard" suite of services,[2] and Century Link's program providing free awareness and clean up services to customers whose systems have been infected.[3]

However, as laudable as these and other similar programs are, much more is going to need to be done to protect our cyber systems. In recent congressional testimony, Dr. Edward Amoroso, AT&T's Chief Security Officer, noted that "national infrastructure, including the communications infrastructure, have always been vulnerable to direct physical attack such as cable cuts, asset theft, and sabotage.... (but) the methods and forms of cyber attacks are continually evolving and this dynamism enables such threats to bypass standard preventive measures such as the application of firewalls and intrusion detection systems strategically placed between the critical system and the Internet at large."[4] Just as the cyber threat has evolved, both government and industry must advance new approaches to cyber defense which will demand new roles and responsibilities for each party.

Whereas the historic relationship between industry and the telecommunications owners and operators was characterized by government setting performance measures often including regulatory authority, this model simply will not work in the fast changing dynamic cyber security space.

The sad fact is that in cyber space, all the incentives favor the attackers. For the most part, cyber attacks are comparatively easy and inexpensive to launch while the potential profits are enormous. Meanwhile, infrastructure operators are inherently a generation behind the attackers. Return on Investment (ROI) is difficult to demonstrate for attacks that are prevented and successful law enforcement is

(Continued on Page 7)

[1] *Cybersecurity: Threats to Communications Networks and Private-Sector Responses: Hearing Before the Committee on Energy and Commerce,* U.S. House of Representatives, 112th Congress, (February 8, 2012) (Statement of Larry Clinton, President and CEO, Internet Security Alliance).

[2] *Cybersecurity: The Pivotal Role of Communications Networks: Hearing Before the Committee on Energy and Commerce, Subcommittee on Communications and Technology*, U.S. House of Representatives, 112th Congress, (March 7, 2012) (Statement of Jason Livengood, Vice President, Internet Systems Engineering, Comcast Corporations).

[3] Ibid. (Statement of David Mahon, Chief Security Officer, Century Link).

[4] Ibid. (Statement of Edward Amoroso, Senior Vice President and Chief Security Officer, AT&T).

Cyber Threat *(Cont. from 6)*

virtually nonexistent. With the incentives massively favoring the attackers we will need to evolve a new approach to cyber security that affirmatively engages both industry and government. Industry is best if focused on innovation and incident-management and government should be focused on awareness and providing incentives for investment that may go beyond normal commercial benefit. Citing Dr. Amoroso once again:

Some cyber security legislative proposals include a variety of regulatory schemes ranging from standardized certification to processes that could result in the imposition of regulatory performance standards. Such proposals are the antithesis of the innovation we need. Moreover, they may have unintended consequences of stifling real cyber security improvements. Cyber adversaries are dynamic and increasingly sophisticated and do not operate by laboriously defined rules and processes. The challenges we face in cyber security simply cannot be solved by imposing slow moving bureaucratic processes on those who build, operate and use cyber space.[5]

Fortunately there is a growing awareness that the traditional regulatory model is a bad fit for securing cyber space and thought leadership in industry, the Administration, and Congress. Now the same consensus is needed to determine what is required to find an alternative 21st century model which will create a sustainably secure cyber system.

In late 2009 The Internet Security Alliance (ISA) proposed a model called the Cyber Security Social Contract[6] which argued that the creation of our Nation's telecommunications infrastructure, including the uneconomic requirements for universal service, was accomplished via a "social contract". In this social contract, policy makers provided the owners and operators of the infrastructure with an economic incentive to build out the network and provide affordable service (at a loss) by essentially guaranteeing the rate of return on private investments in these companies. ISA went on to note that this system not only created the world's leading telecommunications infrastructure through the 20th century but had multiple spin-off benefits for the country including economic growth and national unity.

ISA then argued that a similar Social Contract, albeit with different terms, should be created to stimulate universal investment in cyber security, including potentially non-commercially viable investments to secure the infrastructure, just as it had to build the infrastructure in the first place. ISA argued that the government could deploy a "menu of incentives" for industry to invest more in cyber security which would not have a negative budget impact but could be economically attractive to corporations. Included in this menu would be liability benefits, procurement awards, streamlined regulation, Stafford Act access, SAFETY Act recognition, and insurance deductions.

In 2009, the Obama Administration charged the National Security Council staff to do a 60-day review of our Nation's cyber security which resulted in the publication of the Cyber Space Policy Review (CSPR)[7] in a ceremony presided over by the President at the White House. The first source cited in the CSPR was the Cyber Security Social Contract. Moreover, the white papers that were cited in the Social Contract were also cited in the CSPR making these publications by far the most cited source in the President's signature document on cyber security.

In 2011, House Speaker John Boehner appointed a GOP Task Force to also examine what course the Nation should take to secure cyber space. The Task Force, headed by Mac Thornberry, also came to the same basic conclusion as the CSPR by making its very first recommendation that Congress create a "menu of incentives" to spur cyber security investment.[8] The notion that President Obama

(Continued on Page 14)

[5] Ibid.

[6] Internet Security Alliance, *Social Contract 2.0: A 21st Century Program for Effective Cyber Security*, (2010), available **here**.

[7] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, White House (May 8, 2009), available **here.**

[8] *Recommendations of the House Republican Cybersecurity Task Force*, U.S. House of Representatives (October 5, 2011), available **here.**

Cyber Supply Chain and Utilities Telecommunications Networks – Should the Consumer Care?

by Nadya Bartol, Senior Cybersecurity Strategist, Utilities Telecom Council

A recent hack of Telvent, a maker of smart grid software, demonstrates the brittleness of technology, our heavy reliance on it, and a lack of understanding of the long-lasting impacts such events can have on our daily lives. As reported by multiple media sources, Telvent corporate network was breached, likely by Chinese hackers who installed malicious software and accessed project files for its Supervisory Control and Data Acquisition (SCADA) system. This SCADA system integrates the utility's corporate network with its industrial control systems, and bridges old and new technologies, such as the smart grid. Telvent's SCADA system is used in the electric power, oil, and gas sectors, which provide critical infrastructure for our Nation and its citizens.

This breach could have a serious impact on Telvent's customers' operations and therefore on the Nation's critical infrastructure. Access to the SCADA project files may provide an opportunity for the hackers to study Telvent's technology, create specific malicious code to alter the technology, and implant malicious code into it at a later date. This malicious code can do anything from merely collecting data to activating destructive functionality at predetermined or random points in time. Companies that purchase this tainted technology in the future are likely to be unaware of this "extra" functionality and therefore unaware of the risk that they assume when acquiring it.

Critical infrastructure provides our fundamental needs – power, water, heat (e.g., gas or oil), etc. The systems running those critical functions are increasingly relying on telecommunications networks and information and communication technology components (ICT) such as Telvent's software. The paradox is – what will happen with those telecommunications networks if they don't have power? While telecommunications providers have backup systems, those are finite. Eventually the backup systems will run out. Electric power is fundamental to the modern way of life and to keeping our national critical infrastructure operational. Clean water, heat, and air are fundamental needs that now rely both on the electric power and on the telecommunications networks. The telecommunications sector and the energy/water/gas/pipeline sectors are not just interdependent, they are co-dependent.

Protecting enterprise assets from the "bad guys" who may access these assets via the Internet and internal networks has become a regular business. In contrast, protecting the enterprise from the impact of acquired ICT products and services is a relatively new concept. It is called ICT supply chain risk management (SCRM) and was raised to prominence by the U.S. government between 2006 and 2008. Much progress has been made in developing frameworks and approaches for how this risk can be addressed in government, defense, information technology (IT), and telecommunications. But what about the impact on broader society if the ICT that is compromised is responsible for providing power, gas, or water? The same set of rigorous practices that have emerged for IT and telecommunications should be applied to the underlying ICT running our utilities.

ICT is created globally across extended and distributed supply chains. The longer the supply chain, the less transparent it may become. ICT SCRM (also known as cyber supply chain risk management) is the discipline of protecting the enterprise from the risk created by the extended supply chain of an ICT product or service deployed by an organization. The risk may not materialize until well after the product or service has been purchased and installed into an operational environment within the target enterprise infrastructure. When the product fails or does something even more malicious then simply failing, tracing back to the cause of the problem at that point is likely to be difficult and resource prohibitive. The impact of such a failure may range from a reduction of functionality or

(Continued on Page 9)

Cyber Supply Chain *(Cont. from 8)*

service to a catastrophe, including potentially bringing down the power grid.

Critical infrastructure industries are using increasingly sophisticated technologies and platforms that are connecting to the Internet, such as the smart grid. The cyber supply chain challenge has been focused on government, defense, IT, and telecommunications. The same challenge applies to the communications networks in the utilities industry because of the heavy use of both telecommunications and ICT components. The additional challenge in the utilities industry is the lengthy operational lifecycle of these components and the slower update and upgrade processes adopted by this industry. For example, in the IT industry it is known that a Windows 95 operating system which is more than 20 years old is woefully obsolete, full of vulnerabilities, and should be replaced. It is not uncommon to find even older ICT components in the utilities environment. Once installed, these devices stay operational for a long time.

The good news is that over the last 6 years multiple government and industry groups have engaged to address the problem of cyber supply chain. The frameworks and approaches that have emerged are surprisingly simple in concept but rather complicated to implement. Consensus among these frameworks indicates that substantive progress can be made by explicitly stating cyber supply chain requirements when purchasing ICT products and services. While a number of other specific practices have been identified and documented, one in particular enables the rest– in the necessity for an ICT acquirer to articulate what it needs in clear terms and then monitor what was delivered throughout its operation.

Existing and emerging cyber supply chain standards and best practices address both software and hardware aspects of the problem and can be immediately tailored and applied to the utilities telecommunications context. A short summary of the most mature efforts is provided in the table below:

The energy sector has also begun looking into the cyber supply chain problem, demonstrated by the George Mason University Center for Infrastructure Protection and Homeland Security August 2012 CIP Report. The report highlights the findings and lessons learned from the Workshop on Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity, and Resilience. Further discussion and work is required to validate available practices, tailor them to the utilities sector, and define additional practices if needed. Most importantly, the community needs to increase awareness of the

Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*	Provides 10 key practices for addressing cyber supply chain risk distributed among different stakeholders in the process – acquirer (Federal agency buying ICT product or service), integrator – entity responsible for development, integration, or customization of an ICT system, and supplier – provider of commercial-off-the-shelf (COTS) components to be integrated or customized.
Draft International Organization for Standardization/International Electrotechnical Commission (ISO/IEC 27306), Information Technology – Security Techniques – Information Security for Supplier Relationships	Provides requirements and practices for protecting sensitive information when acquiring products and services. Consists of multiple volumes (parts), with Part 3 addressing ICT supply chain security. Addresses both acquirer and supplier perspectives.
Open-Trusted Technology Provider Standard (O-TTPS)	Provides best practice requirements and recommendations for COTS providers (also known as suppliers).
Software Assurance Forum for Excellence in Code (SAFECode) Framework for Supply Chain Integrity and Overview of Software Integrity Controls	Provides practices and guidance for how to address supply chain concerns in a software development environment.

(Continued on Page 15)

Legal Insights

Guerilla Internet: The Potential Legal Implications of Meshnets

by Christopher Woolley, CIP/HS Research Assistant

There is a growing movement in some corners of the internet to create a meshnet, a separate internet from that which we currently have. This privately owned network would have some properties different from the current internet, including many more private packets of data, and increased private ownership of the means of communication. As such, a meshnet could potentially provide a hurdle to current schemes of enforcement and regulation.

Currently, most of us connect to the internet through an Internet Service Provider (ISP) like Verizon or Cox. The ISP can limit users' connection with the internet, because it owns the means of communication, the software and hardware that connect users to each other. The ISPs can potentially bottleneck information enabling them to restrict usage to individual users. A meshnet places the ownership of the means of communication with the individual user, preventing ISPs from denying access.

The meshnet is something akin to a peer-to-peer network. Every node (a device—computer, smartphone, server, etc.—on a meshnet) is connected to other nodes through some medium, like a cable or wireless connection, and can transmit packages to any specific node on the net via other nodes between the two. Like our current internet, a meshnet allows for multiple paths for a packet through the net. The more nodes, and connections between them, the more resilient the system becomes. The meshnet structure routes packets around broken or damaged nodes. In this way, meshnets are designed to survive the loss of large chunks of the communications infrastructure between points.

There are several meshnet projects in existence, one of which is known as the darknet. The darknet originated on Reddit, a popular aggregate site where users can post about their interests. The idea started as a post in a forum, but has since spawned its own sub-forum with over thirty thousand subscribers.[1] The darknet is being built using the CJDNS packet routing system, a protocol that makes the content of the packet all but inaccessible to everyone except the intended target. CJDNS automatically encrypts the contents of a packet which can then only be decrypted by its intended recipient.[2] On a conceptual level, the system is designed for privacy, not anonymity.

The darknet is set up to run on individually owned hardware and open sourced software. There are currently several large hurdles to a widespread darknet, including the range of personal transmitters for wireless capabilities, the difficulty for wireless hardware in sending and receiving packets at the same time, and the cost and impracticality of using wire as a connection between nodes. Currently, a limited meshnet called Hyperboria is being used as a playground for developers to improve CJDNS programming and experiment with hardware, with the eventual goal of an easy to use, easily put together system of nodes for the darknet.

Should these technical issues be overcome, the FCC may have to redefine its regulations. Promulgated in the fall of 2011, the FCC's net neutrality standards refer to any legal device utilizing any legal content with any legal application on any provider.[3] The existence of a meshnet poses interesting definitional and regulatory challenges to these open internet regulations, which are

(Continued on Page16)

[1] Reddit, DarkNetPlan, with 30,710 subscribers as of 10-31-12, available **here**.

[2] Project Meshnet, available **here**.

[3] United States Federal Communications Commission, Open Internet Guide, available **here**.

Sector Overview *(Cont. from 2)*

the event of disruption

• Improvement to the Sector's NS/EP posture in support of Federal, State, local, tribal, international, and private sector organizations

Selected Accomplishments

Members work collaboratively to maintain and enhance the protective posture of the Communications Sector. Recent Sector accomplishments include:

• Development of recommendations and best practices to ensure the optimal security and reliability of communications systems (including telecommunications, media, and public safety) through the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council (CSRIC).

• Full engagement in joint exercises and training initiatives, including the 2012 National Level Exercise which tested the coordination, authorities, responsibilities, and operational capabilities among U.S. governmental entities, partner nations, and the private sector in response to a significant cyber event.

• Updated collaborative sector documents that include the 2012 National Sector Risk Assessment (NSRA) and the Interim National Cyber Incident Response Plan (NCIRP).

• Improved cross-sector coordination mechanisms to address critical interdependencies through the Telecom/Energy Working Group and the Cross Sector Cyber Security Working Group.

• Coordinated and supported the Network Security Information Exchanges (NSIE), a forum that addresses information sharing, issues surrounding advanced persistent threats, supply chain, and workplace cyber security technology management.

• Completed the National Security Telecommunications Advisory Committee Report to the President on Cloud Computing, which examined the NS/EP implications of the Government's use of cloud computing and included recommendations in areas of strategy, policy and structure, security, and technology.

Key Intitiatives

The Communications Sector continues to promote and improve partnerships that will help government and industry stakeholders prevent, prepare for, detect, mitigate, and respond to a major disruption of critical communications services. Current initiatives include:

• Developing mechanisms to support rapid reconstitution of critical communications services after national and regional emergencies, including cyber security emergencies.

• Working with industry to improve cross-sector coordination mechanisms and address critical interdependencies, including cyber security interdependencies.

• Strengthening continuity of government and operations capabilities across NS/EP users via NCS Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, by participating and testing various continuity mechanisms in government exercises.

• Improving information-sharing programs for government and industry partners at the Federal, State, local, and International levels.

• Providing communications services to mitigate network congestion or disruption via priority services programs such as Telecommunications Service Priority (TSP), Government Emergency Telecommunications System (GETS), and Wireless Priority Service (WPS).

Moving Forward

The Communications Sector is committed to continuing existing partnerships to improve the poster of the communications infrastructure in steady state as well as during an all hazards event. As new threats emerge and as new technologies come online, new partnerships may also emerge. One thing is certain – the resilience of America's communications infrastructure only exists because of the mutual understanding of public and private sector strengths, weaknesses, and opportunities brought about through a commitment to partnerships. ❖

Interoperability *(Cont. from 3)*

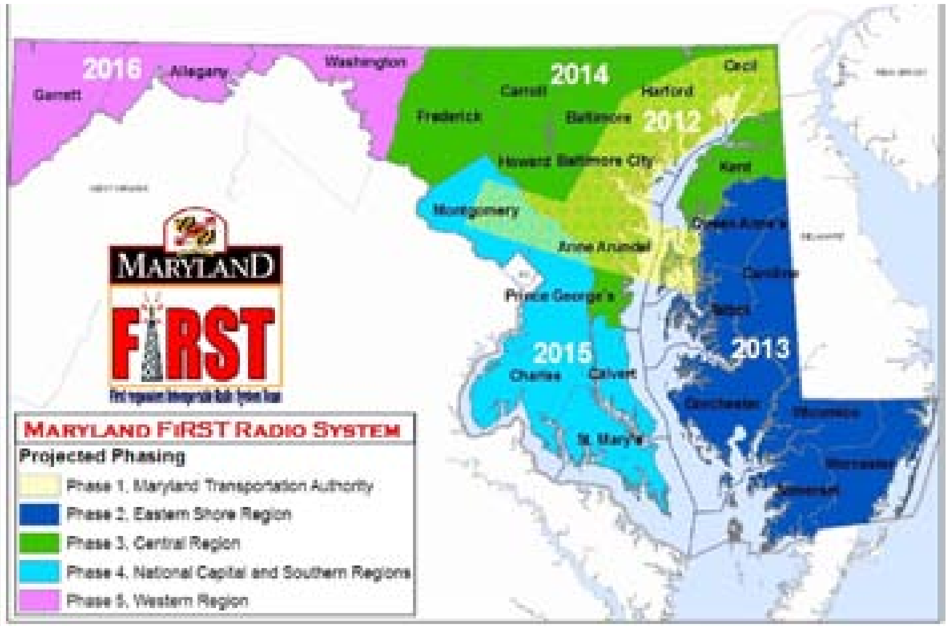
out the success and shortcomings of these plans, and the first responder community adjusted strategies accordingly. One major lesson from the Gulf crisis was the need for resiliency in these systems. Loss of infrastructure such as towers and communications centers along with power outages that lasted for weeks pointed to the need for enhanced construction of critical infrastructure, back-up generators, and mobile units that could be deployed rapidly and a greater focus on continuity of operations.

Are We There Yet?

No, but we're inching closer. Because first responder systems are built and managed on a local basis, it was not practical or economically feasible to throw out the entire public safety radio infrastructure and replace it with a new, nationwide communications system. The first step was to identify spectrum that everyone could use as the common band/s where first responders could operate and communicate without the need for patches. Congress directed the allocation of 700 MHz frequencies that were being used by commercial broadcasters to the States for this purpose. It took years for that conversion to happen but today, Maryland and other States are building statewide networks on this new frequency. The Association of Public Safety Communications Officials also established a set of standards (Project 25 Phase 2) which manufacturers agreed to build on, and which allows any radios built on those standards to talk to each another. The first of those devices became available a couple of years ago.

Building the new infrastructure (towers, shelters, fiber optic, and microwave networks) does not happen overnight. Maryland's new system, known as Maryland FiRST (First responders Interoperable Radio System Team) will take five years to complete, and that is without the cumbersome construction of towers. We are building on radio towers the State built during the last decade while awaiting the 700 MHz frequencies to become available. That was not necessarily a leap of faith. Local counties were given first access to the sites for their local upgrades, and space was reserved for the State system if and when it was built. This month, Maryland will transition the first users to the MD FiRST 700 MHz system. The Maryland Transportation Authority Police, which is responsible for much of the State's critical infrastructure such as the bridges and tunnels along with major interstate highways, will be the first user. MD FiRST will replace the agency's three channel system which does not meet the upcoming FCC requirement for efficient use of spectrum. The new system will give the agency 700 talking groups that cover routine daily activities as well as ones available for special events with any of Maryland's 23 counties, Baltimore City, local sheriffs, fire, EMS, and agencies in the National Capital Region, Delaware, and Pennsylvania.

In this first phase the system will cover two-thirds of the State's critical infrastructure and 45 percent of the population. In addition, we will have one Maryland State Police Barrack along the John F. Kennedy Highway in the northeast portion of the State come onto the system in November, and Kent County, the first local jurisdiction to join the System, will be "on the air" in December. Plans are underway for completion of the entire Eastern Shore in 2013, and we will be seeking legislative funding for the remaining regions this session and next. ❖



Cloud Infrastructure *(Cont. from 5)*

to promote their deployment, operation, and use.

Summary

The security of all mechanisms involved in the communications network is of paramount concern – not only for preventing security threats, but also for enabling damage control and recovery. In response to this need, TIA is taking advantage of existing standards and enhancing the content to provide additional requirements and guidelines that will enhance communications infrastructure protection. The TIA Network Security Task Group effort continues to solicit input from end-users, producers, and general interest stakeholders. ❖

For more information about this effort, visit **here** *or contact* **standards@tiaonline.org**.

SARMA's 6th Annual Conference

focusing on

"Professionalizing Security Risk Management"

on

Tuesday, December 11, 2012 through
Thursday, December 13, 2012

to be held at

George Mason University - Arlington Campus
Founders Hall
3351 Fairfax Drive
Arlington, Virginia 22201

For more information on Registration, Agenda, or Sponsorship, please visit

http://www.cvent.com/events/6th-annual-conference-on-security-analysis-and-risk-management/fees-20a6a8a4c2be4d02b285ed1da83a46c1.aspx.

Cyber Threat *(Cont. from 7)*

and the House Republicans came to similar conclusions on a critical policy approach is, to say the least, unusual.

Unfortunately, the Senate was pushing a more traditional course via the Lieberman-Collins bill which, as introduced, advocated giving DHS extensive regulatory authority over critical infrastructure with respect to cyber security. The Administration abandoned its position in the CSPR and chose to support Lieberman-Collins.

However, by the time the Lieberman-Collins bill reached the floor of the Senate, in the summer of 2012, the DHS authority to impose mandates on the private sector were stripped from the bill and replaced by a rudimentary incentive model. For a variety of reasons, including the lateness of the session and the rigidity of the new approach, it led to the bill not passing. Yet, the fact is that for the first time the Administration, the House, and Senate seem poised to be aligned around an incentive model for cyber security moving forward.

At least some press reports have suggested that the failure of the Senate bill is attributable to partisan politics. However, those closer to the process may see a very different story. First of all, the leader of the opposition to the initial Leiberman-Collins bill was Senator John McCain. Notwithstanding his political stripe, Senator McCain has a long history of bucking his party and the business community in the interests of national defense. If the original Lieberman-Collins bill was truly a good bill, from a security perspective it is highly unlikely that Senator McCain would have opposed it.

Moreover, the Senators who moved the Lieberman-Collins bill from its initial set of regulatory mandates to a more progressive incentive approach were not the Republicans but northeast liberal Democrats, including Senators Whitehouse (D-RI), Coons (D-DE), and Blumenthal (D-CT) in conjunction with less ideological Republicans such as Senator Coats (R-IN) and Senator Snow (R-ME).

Cyber security is a unique issue in many respects, including the lack of legacy models to address it and its swiftly evolving and international nature. Industry and policy makers, quite understandably, are working to create a sustainable model to address this new age problem, and there are signs that a consensus approach is beginning to emerge. ❖

The Center for Infrastructure Protection and Homeland Security Presents:

Fatigue Risk Management in Aviation Operations

The Ongoing Fight for Alertness and Safety

The One Day Session will be held on

January 31, 2013

For more information on Registration and the Agenda **click here**.

Cyber Supply Chain *(Cont. from 9)*

challenge and potential solutions within the utilities sector. That will help ensure that all of us, including the government, defense, IT, and telecommunications industries are able to receive basic functionalities and services, such as having electric power to run those networks.❖

TRACC

Beyond Compliance:
Transnational Crime and Corruption Challenges and Solutions for Executives

This workshop will help anticipating crime and corruption problems executives and their organizations are increasingly faced with in the global setting, developing a forward-looking orientation based on the particular problem, and creating a positive response as part of their corporate culture.

on

November 28, 2012

to be held in

Founders Hall, Room 120
George Mason University - Arlington Campus
Founders Hall
3351 Fairfax Drive
Arlington, Virginia 22201

$ 399 fee includes instruction, materials, and luncheon. Space Limited

To learn more and register, visit http://traccc.gmu.edu

Legal Insight *(Cont. from 10)*

arguably meant to apply to companies providing access to the internet. In a meshnet each user is his or her own provider. They obtain their own hardware and (in the darknet at least) use open source software to connect to other individual users. Depending on how each individual connects his or her node to other nodes, they might use part of the spectrum allocated by the FCC for various purposes. This might raise an enforcement issue, depending on how many nodes were operating in which parts of the spectrum. If meshnets, or specifically the darknet, became widespread, the FCC might have to redefine its standards.

Another, perhaps more obvious issue with meshnets like the darknet is illegal content. It is far easier to communicate illegal content when it cannot be seen by anyone except the intended recipient. The darknet is designed to be private. If a law enforcement agency wanted to gain access to packets sent across the darknet, they would have to be the intended recipient, or obtain a warrant for either the sender or recipient of the packet, as mid-stream interception of the packet would be difficult or ineffective. While law enforcement officials could easily determine the sender and recipient of a packet by gaining access to a node over which the packet traversed, without access to the content of the packet, obtaining a warrant remains a difficult proposition.

The lack of ISPs in a meshnet would also throw a potential monkey wrench into homeland security efforts. ISP cooperation in surveillance is a useful tool in the collective belts of government agencies which would be lacking in a world with widespread meshnets.[4]

It is possible that in the arms race of technology, someone will develop the silver bullet for the darknet or meshnets in general, making the issues raised here completely moot. Some back door to the CJDNS protocol, or an easy method of decryption for example would be a strong blow against the privacy of the darknet. However, lacking such a silver bullet, the efficacy of meshnets will likely not diminish.

There is no widespread meshnet currently; the darknet is still in its infancy, in part because the process of setting up a node on the darknet is so difficult for those unfamiliar with programming and hardware. Widespread use of meshnets may never occur, whether due to the burdensome nature of the initial set up, or for other reasons.
Perhaps current internet users will be overwhelmingly satisfied with the current scheme, and feel no need to switch to a meshnet structure. However, the existence of darknet suggests that at least some people on the margins find meshnets a worthwhile investment of their time, and are working to make them easier to use.

The darknet or meshnets in general are currently not hot topics of discourse, owing mostly to their limited application. However, their growth is a distinct possibility. If the darknet or some other meshnet structure(s) becomes widespread, these issues will have to be addressed. ❖

[4] See, for example, H.R. 6304 (110th): FISA Amendments Act of 2008.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1