

**Congress of the United States  
Washington DC 20510**

Date July 20, 2017  
The Honorable Thomas Wheeler  
Chairman  
Federal Communications Commission  
445 12th Street SW,  
Washington, DC 20554

DOCKET FILE COPY ORIGINAL

From:  
Mr. Jerome Sills-Wha-Dee  
P.o box 2763  
Springfield, MA 01101-2763

Doctoral student/liberty University  
1971 University Blvd., Lynchburg, VA 24515  
Mr. Jerry Farwell presiding president,

Received & Inspected  
JUL 25 2017  
FCC Mail Room

Dear Mr. Chairman:

on July 13, 2017 there was an article posted in the Republican newspaper of Springfield Massachusetts, lawmakers are trying to defend net neutrality and freedom of the Internet, about two dozen congressional lawmakers and others, called for Internet neutrality, apparently, special interest groups are trying to roll back the FCC open Internet order. Many senators have opposed this because it is believed to be a First Amendment right to have a free working Internet, the government is also having problems with cyber terrorists, cyber hackers, and all other types of Internet security threats, there is reason to believe that the companies who actually want to take over and control the Internet, have been providing monies to such cyber terrorists, so that they may form groups in covert operations, for the purpose of penetration and extraction of critical data regardless of location, companies have set up what is believed to be known as cyber underground hubs, where groups of highly skilled computer geeks and experts in cyber war technology, come together and form what you will call, attack teams they take instructions from unknown managers, to penetrate and infiltrate companies and government entities, for the sole purpose to extract information, it has come to the point that security has been hindering their efforts, so now they must take a more direct action and try to control the Internet, so that they can leave back doors open and loop holes in specific Internet areas, for the sole purpose of penetrating and extracting information, whether that information be critical information, personal information or classified information., Now I know this may be hard to believe but you have to say to yourself, who else would actually have the monetary assets to put together a cyber-attack team to penetrate and attack specified targets, paying them in prepaid packages, the exact amounts of payment are not known, but I imagine it's quite generous, considering the risk involved so as the prize that will be obtained at the end, freedom of the Internet means social watch groups can keep an eye on the so-called cyber-attack teams, the cyber-attack teams are global in nature, they can be anywhere, and all that is required is that the companies contact, the

group, In all cases there will be someone to disclose, to activate the attack team, as example, IBM desires to know specified military design secrets that General Dynamics created for the Air Force. This is classified information. However, the cyber attack teams are given enough inside information, possibly security codes and all other types of information that allow them to easily penetrate the air forces security systems extract the information, totally and completely unknown, breaking the FCC laws of network neutrality would mean you would give the bosses of cyber-attack teams and criminals easier access to extract information, and possibly take over the entire government, the amounts of money that they pay are astronomical, for certain specific pieces of information. As the government will not pay this, and this is the reason why you are being defeated, however, I just wanted to do my part by supplying this information, so that you may take countermeasures. I have enclosed additional reports for your review, along with some professional reports that you have already reviewed, some of the materials, provided to you came from the committee on Homeland security and governmental affairs, they had wrote you a previous letter concerning cyber security issues that the United States will be facing now, and in the future, this is not to be taken lightly. As you must realize that the advancement of artificial intelligence combined with quantum fiber-optic computers, will bring a nightmare, and a seriously dangerous condition to the United States, if it gets in the hands a cyber terrorist or cyber attack teams and groups who specifically penetrate and target key targets assigned to them, by companies and corporations right here in the United States and abroad, and informed countries, as a reference. These are the people who have written you and have explained these concerns before the committee on Homeland security, who are as follows.

Committee on Homeland & Governmental Affairs

MICHAEL T. MCCAUL

Chairman

House Committee on

Homeland Security

Cc: The Honorable Jehu Johnson, Secretary, Department of Homeland Security

The Honorable Thomas R. Carper, Ranking Minority Member, Senate Committee on  
Homeland Security & Governmental Affairs

The Honorable Bennie G. Thompson, Ranking Minority Member, House Committee on  
Homeland Security

The Honorable Mignon Clyburn, Commissioner, Federal Communications Commission

The Honorable Jessica Rosenworcel, Commissioner, Federal Communications  
Commission

The Honorable Amit Pay, Commissioner, Federal Communications Commission

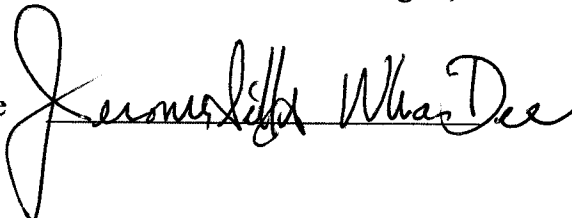
The Honorable Michael Orally, Commissioner, Federal Communications Commission

#### Conclusion

I would hope that you would address this issue on the congressional floor concerning companies who are trying to undermine the Federal Communications Commission by getting them to release control so they can implement a cyber toolbox, that would allow their cyber-attack teams to gain access to critical database and information targets,

Respectfully yours

Jerome Sills-Wha-Dee





Computer security trends, specialty report generated for FCC

Doctoral student information technology specialist

Mr. Jerome Sills –Wha-Dee

Date July 15, 2017

Liberty University

Student number L26996064

### **Purpose and scope**

In discussing the elements of computer security, we turn to a cyber-security planning guide that was published by the Federal Communications Commission. The information in the guide is gathered by a variety of companies that are involved in the cyber security planning process, or otherwise known as the elements of computer security. The scope of this report will be to review the elements involved in computer security, the environment of the topic is related to computer security in general as it will have an effect on government entities, state entities, corporations, commercial businesses, small businesses, university students, and the general public as it is related to using computer systems for basic applications, depending on the user in question.

### **Literature review/investigation**

**The FCC /federal communications commission** has listed, software security providers, as follows, Microsoft, homeland security, the US Chamber of Commerce, McAfee, Symantec, which is a part of Norton security systems and software. FISA Corporation and ADP, a check and processing center that companies use to process payroll checks for employees. In the FCC's planning guide for security there were several issues that are discussed which are as follows, there is discussion concerning privacy and data security, scams and fraud, network security, as well as website security email, mobile devices operational security, and policy development management, along with a list of other cyber security links, and it also has a cyber-security glossary of terms. The FCC basically has gone over the basic requirements for cyber security systems, that cover a cyber-action plan, which includes the following items they first talk about conducting inventory to help you answer the following cyber security questions. Such as what kind of data do you have at your business? Businesses have all kinds of data, some of it more valuable than others, some of it, sensitive, the data, includes customer data and account records,

Transactions, and financial information. Payroll files, Social Security numbers, home addresses, so as you can see this is critical data that must be protected at all times, FCC / federal communications commission. Cyber security breaches and /or cyber security hacks. The second question is how is that data handled and protected. Most small business owners should have a straightforward security plan, the third question is who has access to the data, and under what circumstances, not every employee needs all the information that is in the company's data. As example your marketing staff would need to view employee payroll data, and your administrative staff may not need access to all your customer information. When you do an inventory of data you need to know exactly what type of data you have, and where you keep that data, it's important to assign access to people who require the right type of data, you need to keep a list of specific employees who need specific types of data. Once you have identified your data, keep a record of its location and move it to more appropriate locations that require the data. Privacy is important for any business. Data that is collected on the Internet needs to be protected, your website can be a great place to collect data. You need to create layers of security protecting data, like any other security challenges. You should not rely on just one security mechanism such as a password to protect some sensitive types of data. If that security mechanism fails, you have nothing left to protect your data. It's essential to get a complete inventory so you don't overlook some sensitive data that could be exposed. Another classification is called classified data which is used primarily by the federal government in the elements of computer security, IRS-revenue, **Internal Revenue Service** and security weaknesses, apparently other branches of the federal government have been keeping a close eye on the IRS concerning cyber security, and computer weaknesses that are presently in the system. IRS / internal revenue service center. Based on past reports the IRS's computer system was formal, and hackers stole,

The personal Information of thousands of taxpayers from the Internal Revenue Service website, some years back. Now the Commissioner of the IRS is being questioned about why these cyber security Issues were not corrected. The claim was that computer security has been a problem for the IRS since 1997, the Inspector General said that taxpayers and employee data were the IRS's top management challenge, because of the vast amount of data involved. As a matter of fact the Government accountability office issued a report stating that the IRS still had dozens of weaknesses to its computer system, and it was vulnerable for hacking by outside interference. The problem with the IRS, was because of budget cuts, for denying the agency the ability to upgrade the computer systems, to more advance and secured computer systems. IRS critical, like Social Security numbers, date of birth tax filing status, where they live, this information was previously acquired from another source. The thieves use that information to access the IRS website. See reference information Internal Revenue Service items in the list.

**FBI – federal Bureau of investigation.** Threats, the first thing that the FBI is concerned with is you must keep your firewall turned on. The firewall helps protect your computer from hackers who may try to gain access to your computer to crash it or delete your information, they steal, password sensitive data, anything that's of value in your computer they'll try to get at it, most Norton packages come with this firewall protection, but there are many on the market, the point here is you need some type of firewall protection. The second thing that the FBI says you should have concerning cyber security is to, install or update an antivirus software or program. The antivirus software is designed to prevent malicious software programs from entering your computer, the third thing that the FBI suggested is that you install or update your anti-spyware software. US – CERT – United States computer emergency readiness team.

**United States computer readiness team CERT** – this organization is primarily focused on

Collecting and analyzing data, and distributing that information to federal agencies. The primary mission is to improve the nation's cyber security systems, coordinate cyber information sharing and manage the cyber security risks to the nation, while protecting the constitutional rights of American citizens. The most common malware threat was sanity, which is a full featured application that infects and spreads for the purpose of reliance spam. Another type of computer problem concerned with the CERT is Phishing, Nearly half of all scams originate from three countries, one the United States, two China, and three the Russian Federation. This information is displayed in a ranking from the highest to lowest numbers, of incidences corresponding to the geographical location, from where scams are initiated, 4 elements of computer security that antivirus applications don't protect. Software cannot protect your computer from physical access, and theft, remote threats, peripheral viruses, and phishing, normally a laptop thief will sell the laptop at a later time. Not as a means of obtaining private data, but simply for cash profit.

#### **Framing computer security and privacy: the 1960s and 1970s-Book**

Author Rebecca Slayton published this book in 2016, it basically provides historical perspectives about professional computer security. It defines concepts of computer security and the relationships between computer securities versus privacy concerns. Her book talks about different ways that that computer security was framed beginning around the 1960s and going into the early 80s as a frame of reference, she explains the computer concepts required for businesses and citizens and private users to protect their computer systems, she basically focuses on the common types of intrusions that are normally seen in large corporations and government agencies, the methodologies that are basically used as a means of protection to those who require some computer security, she describes the relationships and architecture of



Computer framing as it is related and mixed with conceptions of professional responsibilities for the security systems involved, and the specific types actions required to enforce those security concepts. Her publication has similar concepts as they are related to computer security requirements for the Federal Communications Commission, the IRS, FBI, and United States computer readiness team.

#### **Understanding computer security author/Etalle, S Sano-Book**

Sano describes concepts concerning popularity and economies of scale, he basically touches upon security aspects of mobile phones that became popular in 2013. His claim is 22% of the world's population utilizes mobile phone technology. The other 20% owns some type of personal PC in Western type societies, mobile phones are the most popular item in their use by more than 50% of the population and also developing countries. He also mentions flexibility and that researchers are utilizing smart phones as study equipment at the micro scale research level, as example smart phones will be utilized on GPS systems so you can find your way around the city in certain cases, there are also being used to monitor people's social and behavior patterns. People voluntarily relay specific types of information that later on may cause them problems. These smart phones are also use to control medical devices implanted in the body such as pacemakers, or other types of biomedical systems which can be easily monitored from long distances and remote locations, security here is critical to protect the patient's medical information. He also relays concepts concerning behavioral sensing is specific types of software and sensors that are built into smart phones, that capture the actions of humans in the form of data,

These types of sensors will measure the behavioral patterns and properties of their users as example, the monitoring of a digital calendar that will generate data patterns of a person's standard work routine, other sensors will indicate how many messages the person received within the day within the week within the month, etc./We can clearly see here that there is a force behind the scenes trying to collect information to learn more about the population which basically is some type of invasion of privacy, you create a lawless society when you keep invading people's privacy's and personal issues, posting additional information on the opportunities and challenges that will be faced, he makes notions to what makes a smart phone. The best and ideal scientific instrument more specifically because it is a portable instrument that can be carried just about anywhere, if allowed, there are security concerns because of the amount of data that these specialty type phones can hold, and they are increasing their sensing and computational capabilities, keep in mind these phones have not come to the quantum level where they will use fiber optics speeds with the utilization of crystal storage memory, which can basically store thousands of terabytes in a single crystal type structure matrix, technology is not there yet, but it is moving at a fast pace, and sooner or later will be at the point where the phones may become too dangerous to carry around, this is the reason why a lot of companies don't allow smart phones in their facilities, all it would take is a smart phone would some type of x-ray scanning device to get into the high security vaults and get proprietary weapons information, or some other type of information that can cause serious problems to countries, not just people entire countries. This is why security is so important.

Computer security is one of the most critical areas on the Internet, and it cannot be overlooked or undermined did, meaning do not take a backseat, or put it in a backseat.

**Computer hacking, security testing, penetration testing and basic security-book**

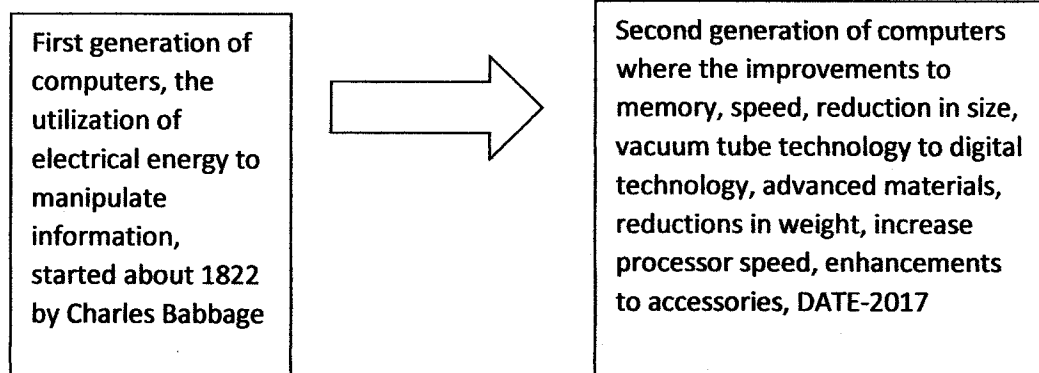
Authors Gary Hall and earn Watson specifically touch upon computer security hacking and prevention, techniques, concerning computer security systems, published December 28, 2016 this publication had over 116 customer reviews, the authors basically go into the primary concerns related to all of the most common types of security problems, as example, they touch upon the different types of hackers and cyber criminals, and the different types of attacks that are utilized by these people. They also mentioned techniques that are used by these hackers for the penetration and/or testing of computer systems. The hacking of Wi-Fi systems, smart phones, laptops, desktops and all other types of computers, including mainframes, servers, and the countermeasures that should be utilized to protect your own personal equipment as well as commercial and government equipment, they touch upon techniques of hacking into computers. If you know how to do this, you can initiate countermeasures to stop it, they also talk about additional aspects of computer security, as well as the future, of the next generation of hackers a potential computer security concerns, the techniques and concepts in this book start from the beginners level and go all the way to intermediate levels and also present concepts at professional mastery levels, personally I would recommend this book to anybody as a reference. If you are involved in computer service and repair or you have a computer and you just want to learn a little more about it. Most of the material being presented here is related to similarly situated conditions that can be found in publications, from the Federal Communications Commission, the Federal Bureau of investigations, letters from United States Congress, homeland security, the United States security computer team, the Internal Revenue Service, the national security agency, state and local police departments, and others,

Computer security fundamentals third edition author William Chuck Eastton 2016-Book

In this publication. William explains the potential threats to your networks and uses basic networking terminology to improve your security systems. And it takes you inside the mental state of a computer hacker so you can develop countermeasures in this publication. William explains the potential threats to your networks. He uses basic networking terminology to improve your security systems and he takes you inside the mental states of hackers, William will identify potential threats. The network use the basics of networking knowledge to implement advanced security systems, he also gives information on counteracting social engineering attacks that are being utilized to get information, then he mentions the most common types of attacks that are utilized such as the Nila, service viruses, worms, spyware, Trojans, malware, etc., he also gives you some insight into the basic technology surrounding computer forensics so that you can compare the different types of technologies for security's that are available, and most importantly, he touches on a lot of other security concepts as well as how cyber terrorism in information warfare are currently evolving, based on my experience I think the most dangerous problem would be the advancement of hardware in the advancement of software as example, in today's society, most computers utilize electrical and electronic systems, that means you have to use a battery or power supply to supply electrical energy to make the computer work. This system is laid out through the entire hardware network of the computer excluding the software or the code that is written to operate the computers, they have advanced in all different types of hardware, and software but they remain at a specified level, that is the electrical level, right now the best computer on the

Market that anyone could purchase would cost anywhere from \$15,000 to about \$30,000. This is practical application, as example. This system would be composed of a system of one or more of the following computers. Primarily laptops or desktops, MacBook's the most expensive hardware piece, that they sell not one, but maybe four or five of them being utilized with the desktop, professional gaming systems like alien ware, three or four of them utilized the desktop. Now these systems go anywhere from five to \$12,000 a piece, so with that in mind if you have the monetary assets you could put yourself a computer bank together and utilize multiple systems at one time. Most people prefer desktops because you can upgrade them easier than you can a laptop, now the primary concern and example here is the level of computer development, in sample one we see a first level computer development, and sample two we see a second level computer development. These are at the basic levels.

### Sample one

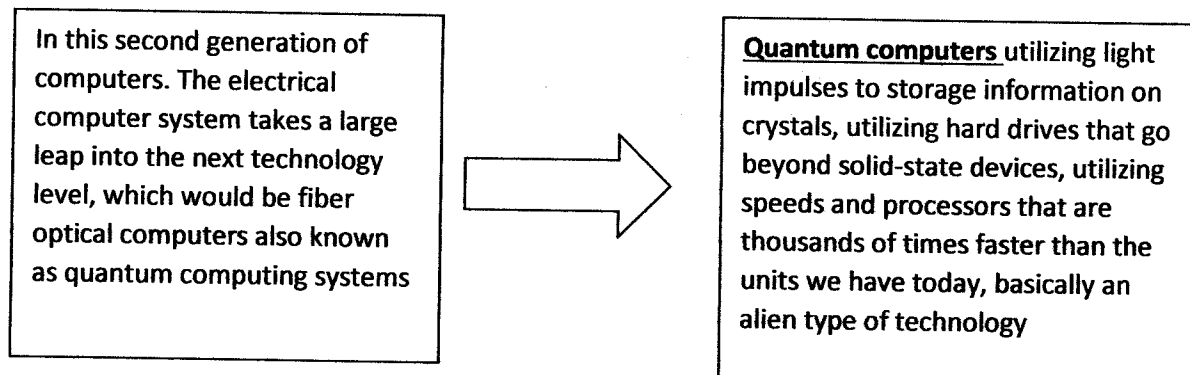


Approximately 195 years have passed since the initial invention of the first computer. This being the case, all these computers up until the present date July 16, 2017 all use the electrical energy still in use today, and all computers being sold by Dell, Hewlett-Packard and all the

Other computer manufacturers around the world. However, a vast problem is on the horizon.

Let's take a look at the potential of the second generation of computers.

### Sample two



In this technology jump the present day technology utilized in electrical or electronic computer systems takes a technology jump into quantum computers that utilize light impulses for greater speed, greater memory storage capacity and greater hacking abilities. These computers oppose the ultimate threat to any type of electrical system because the speeds would be so incredible that no electrical system could keep up with it, even though electrical energy travels at the speed of light, it was still not be as fast as a computer that utilized light impulses and crystal technology. This is the next generation of computer currently being worked upon at the Massachusetts Institute of Technology, California State University, the University of technology in Beijing China and many other universities and private corporations around the world, although quite not there yet. It's only a matter of time and if a hacker or cyber security criminal ever gets their hands on one of these computers. You will have to deal with serious business, so it advise you to be prepared for this, taken into biblical contacts. I don't know the exact

Scripture, but I know it says prepare now for his coming. Because once this type of technology is let loose, your problems will only multiply by thousands of times.

### **Analysis and discussion**

Based on all the information presented in the literature review investigation, the results of this investigation point to the fact that we will require more computer system security specialist in the future as well as hardware and software developers, that will be building or designing advance computer equipment for business and industry, as well as government entities, we will require and it is justifiable to implement better security systems within these new developed technologies, especially if we will be making a technology jump or leap into optical computer systems or quantum computers, which will operate thousands of times more faster than the current electrical based computers of today. As you can see in the drawing samples that I posted in this report, you will note that all computers of today utilize electronic and electrical energy to process information, in the second sample drawing you will see the electrical energy computers transforming into quantum or fiber optical computers, that is the next generation or leap in computer technology, I can even take you one more jump beyond quantum computers, it depends on the type of materials found, there are other materials that will process information faster than optical equipment, but these materials are classified, that would be the third generation, and with the enhancements and combinations of all three types of computers you would have a fourth generation, this fourth-generation would be called artificial intelligence as it would be a living computer system, in a biblical sense, I would be kind of afraid to ask the great Spirit how he felt about this new type of forthcoming.

### Synthesis

Based on all the information that I have presented concerning computer security. My conclusions are as follows. I would recommend taking a closer look at the developing technologies concerning computer advancement, as the computers advance they will require higher levels of security, because they will be more advanced, if the computer systems become more advanced, that means the software systems will have to be more advanced, that means the security systems will have to be more advanced, as example, if the current computer technology utilizes electrical energy, this means it basically works on electricity and electronics and it has specific speeds and capabilities, however they are limited to a specific point at this time, and at this time you are having problems with your computer security, it only seems reasonable that if you make the jump to a quantum computer system which utilizes light impulses which will increase computer speed, and capacity by thousands of times. It will also generate a greater level of security problems, this type of computer is far more advanced than today's computers so you will require more highly skilled people to develop the counter technologies involved, with these quantum computers. This being the reason that these quantum computers have not been released yet, even though they're in there seed stage, my predictions concerning the future events is that once quantum computers become available to anyone that will utilize them. Yes, there will be benefits, but along with benefits there come problems. Problems that will be thousands of times worse than the problems they have today, as example, someone purchases a new quantum computer, and takes it home to his basement or home laboratory, he decides to build a robot or artificial intelligence using this technology. The robot develops a consciousness and decides to build more of itself and take over.



all the information in this report comes down to a few basic terminologies that are similarly situated to all references and they are as follows, all references deal with computer security in its present-day form, all references show how cyber criminals conduct their activities to extract information from your computers, all references show countermeasures to deter cyber criminals, all references show techniques and applications that are utilized for cybercrime as well as to prevent cybercrime, all references referred to the protection of computer systems and networks, all references referred to future events and forecasts that could possibly unfold in future computer security conditions, however, most of them fail to address the fact that we are still utilizing electrical and electronic based computer processing technology. It says nothing about the next leap or jump in technology, and this is the dangerous and critical factor. Once these electronic, electrical based computers go to the next levels, which based on my experience and research would be as follows, electrical, computer systems jump to quantum computer systems which are fiber optical high-speed computers, fiber optical computers jump to artificial intelligence based computers utilizing fiber optical systems, the next jump would be artificial intelligence computers, two biological artificial intelligence fiber optical based computers, otherwise known as Artificial life forms living computers, today's technology is having a hard time dealing with the problems from these basic electrical or electronics based computers. How you could possibly expected deal with the next level, which is quantum computers. Never mind the other levels. These technology areas require more in depth doctoral research work so that we may have the ability to forecast the future problems associated with these technologies.

**Forecast model**

12. New teachers arrive on earth from distant world's government powerless to intervene?
11. Forgiveness will humans be forced to leave the planet because of their past actions?
10. Judgment day. Have we gone too far/do we explore the heavens the unknown? 2090
9. The Great Spirit makes an appearance/concerning the new life forms 2080 to 2090
8. AI computers do research on themselves and develop bodies of pure energy 2070 to 2080
7. AI computers develop super superior bodies/humans want the bodies 2060 to 2070
6. AI computers develop consciousness and start to self-develop their systems. 2050 to 2060
5. Artificial intelligence fiber optical/biological computer systems go online 2041 to 2050
4 artificial intelligence/AI fiber optical computer systems go online 2030 to 2040
3 quantum fiber optical computer systems go online 2017 to 2030
2. Electrical computer systems currently in use. 2017
1. First computer developed 1822

### References

1. [www.fcc.gov](http://www.fcc.gov) /Federal Communications Commission
2. [www.irs.gov](http://www.irs.gov)/Internal Revenue Service Ctr.
3. [www.fbi.gov](http://www.fbi.gov)/federal Bureau of investigation
4. [www.computer readiness team/](http://www.computer readiness team/) United States.gov
5. Framing computer security and privacy, the 1960s and the 1970s author of Rebecca Slayton newsletter published November 3, 2016. ACM, New York, New York, USA.  
ACM computers and Society archives doi-10-1145/3024949.3024945
6. Title: understanding computer security authors:Etalla, sano Journal title: frontiers in ICT  
I SSN: 2297 – 198X date 2014, volume 1,
7. Hacking, computer hacking, security testing, penetration, testing and basic security  
December 28, 2016 authors Gary Hall author Erwin Watson. ISBN number  
9781541289321/116 customer reviews
8. computer security fundamentals third edition publication date 2016 authors William  
Chuck Easton, 21 customer reviews/ISBN number 13 – 978 – 0789757463 alternative  
ISBN number ISBN 10 – 078975746X

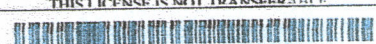
**Congress of the United States  
Washington DC 20510**

July-21-2017  
The Honorable Thomas Wheeler  
Chairman  
Federal Communications Commission  
445 12th Street SW,  
Washington, DC 20554

Dear Mr. Chairman:

Important references related,

I currently hold an FCC Marine radio operator permit, I have passed element eight of the license requirements for FCC license, I am currently working on passing the final element to receive full radiotelephone operator license, as it is awarded by the Federal Communications Commission.

UNITED STATES OF AMERICA FEDERAL COMMUNICATIONS COMMISSION			
Marine Radio Operator Permit			
ATTN: JEROME SILLS, JEROME 31 HAWTHORNE STREET SPRINGFIELD, MA 01105			
FCC Registration Number (FRN): 0025207507			
Special Conditions / Endorsements			
License authorized lifetime status pursuant to Memorandum Opinion and Order, Third Report and Order, and Third Further Notice of Proposed Rule Making in FCC 06-129.			
 FCC-REGISTRATION-NUMBER-0025207507			
Grant Date	Effective Date	Print Date	Expiration Date
02-21-2017	02-21-2017	02-22-2017	
File Number	Serial Number		Date of Birth
0007669691	MP00038326		06-03-1964
THIS LICENSE IS NOT TRANSFERABLE			
 Jerome sils - Kha-Dee (Licensee's Signature)			
FCC 605-FRC - May 2007			

**Congress of the United States  
Washington DC 20510**

JUN 23 2015 stamped by FCC

June 17, 2015  
The Honorable Thomas Wheeler  
Chairman  
Federal Communications Commission  
445 12th Street SW,  
Washington, DC 20554

Dear Mr. Chairman:

As you are aware, our Nation faces a considerable cyber threat. That threat continues to grow in terms of both sophistication and frequency, from foreign state actors, criminals, hackers, and terrorists who will not hesitate to steal, destroy, or vandalize our cyber assets. Cyber criminals can utilize a variety of techniques to gain access to our computer networks. But wireless networks are particularly vulnerable to attack. Because wireless networks are ubiquitous-present in homes, businesses of all sizes, restaurants, hotels, and airports-and do not require physical access for a connection, securing them is a unique challenge. For example, wireless networks are especially vulnerable to man-in-the-middle attacks, denial of service attacks, and eavesdropping.<sup>1</sup>

No one is immune from cyber incidents, as evidenced by recent intrusions at JP Morgan Chase, Anthem, Home Depot, Target, the White House and, most recently, the Office of Personnel Management. To protect our Nation and its citizens, the Federal Government must be a leader in best practices on cybersecurity and ensure the legal and regulatory environments our businesses operate in provide them the flexibility they need to secure their networks against attack. In discharging that leadership role it is imperative that government agencies give consistent guidance and support to businesses in meeting and defeating cybersecurity threats. Unfortunately, we are concerned this goal is not being met due to conflicting information from the Department of Homeland Security (DHS) and the Federal Communications Commission (FCC) regarding the use of Wireless Intrusion Detection Systems and Wireless Intrusion Prevention Systems (WIDS/WIPS) to protect wireless networks and users from cyberattacks.

<sup>1</sup> See, e.g., MURUGIAH SOUPPAYA & KAREN SCARFONE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-153, GUIDELINES FOR SECURING WIRELESS LOCAL AREA NETWORKS (WLANS) (DRAFT) 8-9 (2011).

The Honorable Thomas Wheeler

June 17, 2015

Page 2

In September 2011, DHS's National Cyber Security Division issued the *Wireless Local Area Network (WLAN) Reference Architecture* in which it discussed the importance of WIDS/WIPS. Because WIDS/WIPS can "detect" and "take countermeasures against the WLAN [wireless local area network] threats," the reference architecture concluded that "WIDS/WIPS deployment is critical to the WLAN security and operation, and therefore is required by the WLAN Reference Architecture." 3

However, on January 27, 2015, the FCC's Enforcement Bureau issued an Enforcement Advisory which suggests that a WLAN operator violates federal law when using WIDS/WIPS to "block" a wireless network access point that is being used to launch a cybersecurity attack against the operator's network or its customers.<sup>4</sup> The agency also intimated that equipment with



WIDS/WIPS functionality is the equivalent of "jammer," the operation of which is unlawful.<sup>5</sup> To better understand the coordination between the FCC and DHS and other agencies on this Matter, and your position on use of WIDS/WIPS to protect networks against cyber-attack, we Request you provide answers to the following questions:

**Interagency Coordination**

(1) With what other agencies, including DHS and the National Institute of Standards and Technology (NIST), did the FCC coordinate in developing the Enforcement Advisories referenced above and how did it coordinate with those Agencies?

**Consistency with Existing Federal Cybersecurity Initiatives**

(2) The *WLAN Reference Architecture* "offers best practices" for WLAN security. Is there any policy reason the private sector should not be encouraged to follow DHS's guidance in protecting their networks?

(3) What recommendations would you offer to a WLAN operator in the private Sector about the use of WIDS/WIPS in protecting its network from Cybersecurity threats, given the apparent conflict between DHS's *WLAN Reference Architecture* and the FCC Enforcement Advisories referenced above?

<sup>2</sup>DEPT OF HOMELAND SEC. NAT'L CYBERSEC.DIV., WIRELESS LOCAL AREA NETWORK (WLAN) REFERENCE ARCHITECTURE § 4.4 (2011).

<sup>3</sup>LD.

<sup>4</sup>Fed. Comic's Common, DA 15-113, Enforcement Advisory: WARNING: Wi-Fi Blocking is Prohibited (Jan. 27, 2015).

<sup>5</sup>See Fed. Comic's Common, DA 12-347, Enforcement Advisory: Cell Jammers, GPS Jammers, and Other Jamming Devices (Mar. 6, 2012).

The Honorable Thomas Wheeler

June 17, 2015

Page 3

(4) Would the use of WIDS/WIPS to detect and stop a cybersecurity threat be Consistent with the use of mitigation efforts "to prevent expansion of an event, Mitigate its effects, and eradicate the incident," as recommended in the NIST *Framework for Improving Critical Infrastructure Cybersecurity's*

(5) Would the use of WIDS/WIPS to detect and stop a cybersecurity threat be Consistent with the use of "Intrusion Detection-Protection" to prevent, mitigate, Respond, and recover from "cyber-attack incidents," as recommended in the Communications Security, Reliability, and Interoperability Council's *Cybersecurity Risk Management and Best Practices* report?"

**Permitted and Non-Permitted Uses of WIDS/WIPS**

(6) Under what circumstances is the use of WIDS/WIPS permitted and under what Circumstances is it prohibited?

(7) If a malicious actor sets up a wireless network access point designed to spoof Another, legitimate access point in order to steal personal information from users Of the legitimate access point, is the operator of the legitimate access point Permitted to use WIDS/WIPS to block that access point and thereby protect Unsuspecting users from associating to it?

(8) If a malicious actor sets up a wireless access point that is being used to launch Attacks against another wireless network, is the operator of the wireless network Being attacked permitted to use WIDS/WIPS to block that access point in order To protect its network?

(9) Are Federal agencies operating WLANs required or advised to utilize WIDS/WIPS to protect their networks from cybersecurity incidents? If so, why Should the private sector be prohibited from using the same technology to? Protect their networks from cybersecurity incidents?

We request your responses to these questions as soon as possible, but no later than 5:00 p.m.  
On July 2, 2015.

<sup>6</sup> NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE  
CYBERSECURITY<sup>34</sup> (2014) [hereinafter NIST CYBERSECURITY FRAMEWORK] (Mitigation RS.MI).

<sup>7</sup> COMM'N SEC., RELIABILITY AND INTEROPERABILITY COUNCIL, WORKING GROUP 4, CYBERSECURITY RISK  
MANAGEMENT AND BEST PRACTICES: FINAL Report 296-30 1, 308 (2015) [hereinafter CSRIC BEST PRACTICES].

<sup>8</sup> For example, a malicious actor might setup a wireless access point in a hotel with the name of the hotel as part  
Of the access point name (SSID) or use a spoofed MAC address of a valid station or access point in the hotels  
Network, to deceive users into thinking the hotel is operating the access point and connecting to it.

The Honorable Thomas Wheeler

June 17, 2015

Page 4

If you have any questions about this request, please contact William McKenna of Chairman  
Johnson's staff at (202) 224-3288 or William McKelma@hsgac.senate.gov and Brett DeWitt of  
Chairman McFaul's staff at (202) 226-8417 or Brett.DeWitt@mail.house.gov. Thank you again  
For your assistance in this matter.  
Sincerely,

Committee on Homeland  
& Governmental Affairs  
MICHAEL T. MCCAUL  
Chairman

House Committee on  
Homeland Security

Cc: The Honorable Jehu Johnson, Secretary, Department of Homeland Security  
The Honorable Thomas R. Carper, Ranking Minority Member, Senate Committee on  
Homeland Security & Governmental Affairs

The Honorable Bennie G. Thompson, Ranking Minority Member, House Committee on  
Homeland Security

The Honorable Mignon Clyburn, Commissioner, Federal Communications Commission  
The Honorable Jessica Rosenworcel, Commissioner, Federal Communications  
Commission

The Honorable Amit Pay, Commissioner, Federal Communications Commission  
The Honorable Michael Orally, Commissioner, Federal Communications Commission