New Threats and Countermeasures in Digital Crime and Cyber Terrorism

Maurice Dawson
University of Missouri–St. Louis, USA

Marwan Omar
Nawroz University, Iraq

A volume in the Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Managing Editor: Austin DeMarco
Director of Intellectual Property & Contracts: Jan Travers
Acquisitions Editor: Kayla Wolfe
Production Editor: Christina Henning
Development Editor: Brandon Carbaugh
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

New threats and countermeasures in digital crime and cyber terrorism / Maurice Dawson and Marwan Omar, editors.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4666-8345-7 (hardcover) -- ISBN 978-1-4666-8346-4 (ebook) 1. Computer crimes--Prevention. 2. Cyberterrorism--Prevention. 3. Computer security. I. Dawson, Maurice, 1982- II. Omar, Marwan, 1982-
HV6773.N4745 2015
005.8--dc23

2015006753

This book is published in the IGI Global book series Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) (ISSN: 2327-0381; eISSN: 2327-0373)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 6
Legal Issues:
Security and Privacy with Mobile Devices

Brian Leonard
Alabama A&M University, USA

Maurice Dawson
University of Missouri – St. Louis, USA

ABSTRACT

Privacy and security are two items being woven into the fabric of American law concerning mobile devices. This chapter will review and analyze the associated laws and policies that are currently in place or have been proposed to ensure proper execution of security measures for mobile and other devices while still protecting individual privacy. This chapter will address the fact that as the American society significantly uses mobile devices, it is imperative to understand the legal actions surrounding these technologies to include their associated uses. This chapter will also address the fact that with 9/11 in the not so distant past, cyber security has become a forefront subject in the battle against global terrorism. Furthermore, this chapter will examine how mobile devices are not like the devices of the past as the computing power is on par with that of some desktops and the fact that these devices have the ability to execute malicious applications. In addition, this chapter will discuss the reality, significance, legal and practical affects of the fact that suspicious programs are being executed offensively and security based attacks can be performed as well with the use of programs such as Kali Linux running on Android.

LEGAL BACKGROUND

Privacy and security are two ideals that are woven into the very fabric of the United States (U.S.) law. This is evidenced by the fact that they are principles that are embodied in the U.S. Constitution (*U.S.* Const., 1787). However, supporting and protecting these ideals is not without challenge, especially as technology and innovation make it increasingly more difficult to navigate these ideals and to continue to protect them. In a post-9/11 era, privacy and security have become increasingly challenging and in some cases have become difficult to reconcile with one another. One such area, is that of the safety and security of the Internet, including the mobile devices that are used more and more to access and

DOI: 10.4018/978-1-4666-8345-7.ch006

transact business and personal matters via the Internet. The dilemma faced by the U.S. is attempting to provide for the protection of the U.S. and its citizens from cyber attacks on the one hand, and trying to ensure that in so doing, the U.S. government does not become too intrusive into the lives of individuals and businesses on the other hand. This difficulty is most likely the reason why the U.S. still has yet to develop consistently broad national policy regarding cyber-security and the protection of U.S. citizens from cyber attacks. Moreover, the swiftness with which technology changes, and new threats emerge, have made it even more difficult for U.S. law and policy to develop comprehensive safeguards to protect the nation's and it's citizens' secure information.

INDUSTRY-SPECIFIC LAWS

Although comprehensive policy remains a challenge, there have been strides made in the passage of laws in specific industries and areas where the U.S. government and by representation, most U.S. citizens have acknowledged and likely accepted the need for national regulation regarding the security and safety of information. An early attempt at protecting electronic information from unauthorized access, is the Electronic Communications Privacy Act ("ECPA"). This Act criminalizes the unauthorized access of the electronic communications of another without the owner's or recipient's permission (Electronic Communications Privacy Act, 1988). Although probably not contemplated by the Act in its inception, mobile devices which transmit electronic communications in the form of e-mail and other forms of communication are likely covered by the ECPA (Electronic Communications Privacy Act,1988). However, this Act does not go far enough in that it does not deal more specifically with the more sophisticated nature of cyber attacks today.

Next, health information is probably for many the most important area of information that needs protection from attacks. Through the Health Insurance Portability and Accountability Act ("HIPAA"), the U.S. Government has provided for the creation of national standards for both the practical and technical security of health information (Health Insurance Portability and Accountability Act, 2000); Security Rule and Privacy Rule, 2003). Through subsequent standards adopted by the U.S government, these technical standards include such safeguards as the use of encryption, passwords, and other means of protecting health information from cyber attacks (Health Insurance Portability and Accountability Act, 2000; Security Rule and Privacy Rule, 2003).

Furthermore, post 9/11, the U.S Government formed the Department of Homeland Security through the Homeland Security Act ("HSCA"). Among other things, this act requires steps to be taken to protect it from terrorist attacks to include cyber attacks (Homeland Security Act, 2006). The Act provides for standards to protect the nation's defense network as well as to share information with private industries and organizations to protect against cyber threats in the private sector (Homeland Security Act, 2006). Along with the HSCA, the Federal Information Security Management Act ("FISMA"), requires all federal agencies to take measures to protect their networks, electronic information, and devices from cyber attacks (Federal Information Security Management Act, 2006). Lastly, the Gramm–Leach–Bliley Act ("GLB") requires banks and financial institutions to maintain the security of financial information and transactions (Gramm–Leach–Bliley Act, 2000).

As is clear from their industry-specific application, outside of national security and defense (HSCA), health services (HIPAA), federal agencies (FISMA), and financial services (GLB), all of these measures fall short in providing for comprehensive reform and policy regarding the protection of individual users of mobile devices and other devices from cyber attacks.

CURRENT CYBER-SECURITY EFFORTS ANDTHREATS

The U.S. government has identified multiple risks associated with cyber terrorism and its impacts. Cyber warfare is not limited to computer grid systems but all systems that are vulnerable such as mobile devices. Lewis (2002) states that the literature on cyber security assumes that the associated vulnerabilities of critical infrastructures and computer networks are the same.

FEDERAL EFFORTS

To that end, there have been some efforts by the U.S. government to deal with the area of cyber-attacks and cyber-security measures. Under his executive authority, for example, the President has issued an Executive Order - Improving Critical Infrastructure Cybersecurity (Executive Order No.13636, 2013) (the "Order"). This Order provides for among other things, information sharing among federal agencies and with the private sector, to include dissemination of reports regarding critical infrastructure assets, consultation, civil liberty protection, critical infrastructure risk reduction, cyber-security framework development, voluntary cyber-security program creation, and critical infrastructure cyber-security risk identification (Executive Order No.13636, 2013).

As required by the Order, the document, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0,(the "Framework") was developed and issued within one year of the Order, on February 12, 2014. In 41 pages the Framework addressed the issues outlined by the Order (National Institute of Standards and Technology, 2014). The Framework makes clear that it is a living document and due to the constant changing nature of cyber threats that may occur, the Framework would also need to evolve and remain a fluid document (National Institute of Standards and Technology, 2014). The Framework's Core elements are Functions, Categories, Subcategories and Informative References (National Institute of Standards and Technology, 2014). The Functions of the Framework's Core are to Identify, Protect, Detect, Respond, and Recover (National Institute of Standards and Technology, 2014).

After research, it was determined that three agencies, the Environmental Protection Agency ("EPA"), the Department of Health and Human Services ("HHS"), and the Department of Homeland Security ("DHS") were required to submit reports regarding their specific areas of critical infrastructure ("the Reports") (*Assessing Cybersecurity Regulations*, 2014). The White House). The DHS report was comprised of three (3) areas: maritime critical infrastructure cyber-security standards, chemical facility anti-terrorism standards, and transportation critical infrastructure cyber-security standards (U.S. Department of Homeland Security, 2014). The EPA report focused on water and wastewater critical infrastructure cyber-security standards, and the HHS report focused on food and drug critical infrastructure cyber-security standards, and cyber-security standards and exercises designed to handle attacks on medical devices and health organizations. (U.S. Department of Health and Human Services, 2014,) While the federal government acknowledges that there is still more work to do, it is proud of the progress it has made in the area of cyber-security measures for critical infrastructure (The White House, 2014).

While the Order, the Framework, and the Reports are an important step toward national policy on cyber-security, they are limited to those areas considered critical infrastructure, or those areas and/or industries, both physical and virtual, that are "...so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters..." (Executive Order No.13636,

2013). There is a pretty good chance that use of smartphones, tablets, or other mobile devices might not fall into that category. In addition, even in the case of critical infrastructure, the Order specifically excludes any regulation of critical infrastructure security beyond what is already existing under current law, meaning, that it only requires certain actions to be taken but does not provide for greater policy or legal protection than what is already provided by other laws. Moreover, since it is only an Executive Order, it is applicable only to the federal agencies under the executive branch of government's control anyway (Executive Order No.13636, 2013).

STATE EFFORTS

In order to have significant, comprehensive and national policy regarding cyber-security for mobile devices, it is without question, a matter that the U.S. government is likely better equipped to handle and address. However, state efforts are still important and can be useful in this area. Not surprising, for example, the state of California has taken measures to include the passing of a law requiring businesses and organizations that experience a security breach to provide notice of the breach to those affected (Notice of Breach of Security Act, 2003). In addition, the state of California has also passed a provision requiring that businesses that maintain users' secure information, to enact "reasonable" levels of security to prevent the unauthorized access or disclosure of that information, which includes protection from cyber and other attacks on such information (California Assembly Bill No. 1950, 2004). As with the federal initiatives, it is likely that even these steps alone are not sufficient to protect users of mobile devices from cyber attacks.

However the state of California's Attorney General's Office has issued certain public awareness campaigns aimed at helping its citizens protect against cyber attacks using mobile devices. For example, its "Getting Smart about Smartphones" Campaign provides information sheets with Tips for Parents and Tips for Consumers. These information sheets warn parents and consumers of the risks of Apps, and encourages the screening, controlling, and reporting of Apps, as California law requires Apps to have a privacy policy (State of California Department of Justice Office of the Attorney General, 2013,). Furthermore, the Tips for Consumers remind consumers to not only check their Apps, but to check their Network, and that just like the desktop computer, smartphones remain vulnerable to attack from spyware, malware, and hackers. (State of California Department of Justice Office of the Attorney General, 2013, State of California Department of Justice Office of the Attorney General) Similar campaigns could go a long way to inform and educate users of mobile devices about the risks of cyber attacks.

PROPOSED REGULATIONS

Unfortunately, the lack of a national uniform policy regarding cyber security of mobile and other devices largely exists due to the lack of consensus in the U.S. government on the best way to provide such security and protection and at the same time avoid over-involvement of government in citizen's private affairs. This can be see in the failure of legislative efforts on both sides of the isle in Congress and by the President. For example, the Cyber-Intelligence Sharing and Protection Act (CISPA) was passed by the House of Representatives, but not favored by the Senate or the President, over concerns that in requiring the sharing of information, it also failed to protect critical infrastructure, as well as waived several civil liberties and

threatened individual privacy. (Cyber-Intelligence Sharing and Protection Act, 2012; Lardinois, 2012,). Similarly, the Cyber-security Act of 2012 was passed by the Senate and had Presidential support, in an attempt to provide for greater protection from cyber-security attacks. However, just like the CISPA, this bill faced opposition, largely due to concerns over the bill's alleged increased regulation of businesses. (Cybersecurity Act, 2012; *Cybersecurity Bill Wins Key Senate Vote*, 2012).

MODEL NATIONAL POLICY

Despite the failed legislative efforts to adopt national legislation and policy regarding cyber-security for mobile and other devices, there appears to at least be a consensus among the federal legislative and executive branches, of the necessity to enact some federal provision dealing with cyber-security in general. Given the importance and frequency of use of smartphones, tablets and other devices, any federal provision dealing with cyber-security would also most assuredly need to address mobile device security. This is because, as indicated by California's Attorney General, for the purposes of cyber-security, mobile devices are just as vulnerable as desktop computers and similar devices to attack. The main impediment then is what shape such regulation should take, taking into account the individual civil liberties and privacy concerns, business regulation concerns, and the protection of critical infrastructure concerns.

At the outset, a theoretical model policy on cyber-security for mobile and similar devices, would most likely need to emanate from the federal government. While each state has an interest in developing its own policy, a national policy would likely be more consistent and easier to navigate for most consumers and businesses, rather than a state by state approach. Furthermore, a national model policy on cyber-security likely has legal support and is authorized by the U.S. Constitution, under the Commerce clause' s authority to regulate matters that travel in or affect interstate commerce, which would include not only e-commerce but the use of mobile devices almost by definition (*U.S. Const.* 1787). Furthermore, there are likely numerous federal statutes and federal agencies that provide a basis for and could enforce a national model policy on cyber-security for mobile devices. However one possible agency that could be utilized in this national model policy is the the Federal Trade Commission ("FTC"), which was created by and enforces the Federal Trade Commission Act ("FTA"), and other rules promulgated by the FTC.

The FTC seems to be a wise choice not only for enforcing such a model national policy on cyber-security on mobile devices, but it also can assist in evaluation and implementation of such a model national policy. This is because as a bipartisan independent agency, the FTC is uniquely suited to handle the various disputes that have plagued Congress and the President in attempting to come to a consensus about the larger issue of cyber-security and the smaller issue of cyber-security for users of mobile devices. (Federal Trade Commission Act, 1914) Moreover, one of the FTC's primary roles is consumer protection. Consequently the most likely victims of cyber-security attacks and breaches upon mobile devices are consumers, and thus the agency charged with protection of consumers seems to be the likely choice to promulgate and enforce standards of a national model policy to address this issue. Furthermore, the FTC has already taken steps to protect consumers from cyber-attacks through cases it has presented against Twitter and Wyndam, for example. (U.S. Federal Trade Commission, 2011; Egan, 2014).

In addition, the FTC could engage in public education and awareness campaigns designed to assist consumers in becoming more knowledgeable about the existence of and how to prevent cyber attacks similar to those used by California's Attorney General's office mentioned above. While the FTC can develop specific standards, through the public comment and hearing process, there still needs to be a

national model policy which lays the framework for the FTC to utilize. The good news is that there is already a starting point for such a framework in place. However, the Framework developed as a result of the Order issued by the President would need to be expanded to include consumer protection and more specifically the threat of cyber-security attacks on mobile devices used by consumers in order to be developed into a national model policy. This can likely be done with the aid of the FTC, as well as private entities or public interest organizations committed to protecting and ensuring the integrity of mobile devices for their continued use. Once the consumer protection and mobile device provisions are added to the Framework, the final pieces to be added would be provisions to protect individual privacy and business autonomy, which could follow the previous examples of HIPAA and GLB, since these laws are industry-specific, to address such concerns. Critical infrastructure protection is already provided for in the Framework and thus this concern has already been addressed by the document. Once completed, the revised Framework would still need bipartisan support from both houses of Congress and the President, before being adopted. If that can be done, then the U.S. could finally have a national model policy on cyber-security for mobile devices. The national policy could allow states to model their own policy after the national policy, where necessary, but could retain certain minimum standards necessary to ensure continuity and comprehensiveness nation-wide.

Finally, as always the courts as the third and final branch of the federal government would serve their ever-important role of interpreting such provisions of the national policy to ensure that the privacy and other legal concerns are adequately protected as they have done in the past, while still preserving the ideal of cyber-security for consumers using mobile devices (*U.S. Const.*, 1787; Marbury v. Madison, 1803).

GOVERNMENT TECHNICAL GUIDANCE

The National Institute of Standards and Technology (NIST) is charged with promoting innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance America's economic security. Additionally, it is charged with improving the quality of life. NIST's Computer Security Division publishes the Special Publications (SP) 800 Series that are general interest to the computer security community. These publications represent collaborative efforts between industry, government, and academia. NIST Special Publication (SP) 800-124, Guidelines on Cell Phone and PDA Security provides general insights into securing these devices (Jansen & Scarfone, 2008). Jansen and Scarfone (2008) provide guidance about the threats and technology risks associated with mobile devices to includes potential methods for mitigation. Ayers, Brothers, and Jansen (2013) drafted guidelines for mobile forensics which is important as the U.S. has the right to use forensics techniques at any port of U.S. entry at that particular entry point. An older guidelines NIST SP 800-19 Mobile Agent Security, published Oct 1999, was one of the first guidelines to address security for mobile agent security. Jansen and Karygiannis (1999) identified generic security objectives and various measures for countering the identified threats. It is important to note that the SP 800-19 address specifically mobile code execution.

Other key NIST guidance such as SP 800-164 Guidelines on Hardware-Rooted Security in Mobile Devices provide guidance on how mobile devices can provide strong security assurance to end users and organizations (Draft) (Chen et al, 2012). The aim of the guidance document is to further industry efforts to implement these primitives and capabilities (Chen et al, 2012). As much of the other NIST SPs this SP provides a baseline of security technologies that can be implemented that will aid in securing mobile devices that are used in enterprise environments. The key capabilities in this SP is broken into three sec-

tions which are the following: 1) device integrity, 2) isolation, and 3) protected storage. Device integrity is the absence of corruption in the firmware, hardware, and software in a mobile device. Integrity is one of the three pillars in the Availability, Integrity, and Confidentiality (AIC) triad that Information Assurance (IA) is built upon. Isolation prevents unintended interaction between Information Owners on the same device (Chen et al, 2012). The Information Owner is not to be confused with the Device Owner. Protected storage deals with preserving the confidentiality and integrity of the data while in use, and at rest. However encrypting data has ramifications such as being jailed in certain countries for refusal to give up encryption keys.

Bring Your Own Device (BYOD)

Understanding the legal issues and ramifications are ever more important as organizations are pushing for Bring Your Own Device (BYOD) and security and privacy are a significant factor (Miller et al, 2012). When we think of mobile devices it is essential that the hyperconnectivity trend is taken as a factor (Dawson et al, 2014). As mobile devices connect with corporate networks while still enabling services such as Bluetooth pose a real threat. To be secure and compliant organizations must re-evaluate their wireless security models (Welch & Lathrop, 2003). BYOD will need to address licensing as virtualization must occur for partitioning and security. BYOD has yet to address issues surrounding a data link or confidential data bleed over. An approved architecture must be created to satisfy the policies and laws of that state. Furthermore this architecture must be scalable.

CONCLUSION

In conclusion, legal issues in the area of cyber-security and privacy with respect to mobile devices will have to be continually reviewed and updated where necessary to address and adapt to the changing technological environment. However, a model national policy that provides legal protection, provides for legal standards, promotes education, and information sharing, would be an important and critical first step to protecting consumers and users of mobile devices from the ever-present threat of cyber attacks. Changing trends such as BYOD will force organizations to determine how data is secured and segregated.

REFERENCES

Ayers, R., Brothers, S., & Jansen, W. (2013). Guidelines on Mobile Device Forensics (Draft). *NIST Special Publication*, *800*, 101.

California Assembly Bill No. 1950, (2004). Cal. Civ. Code § 1798.82

Chen, L., Franklin, J., & Regenscheid, A. (2012). Guidelines on Hardware-Rooted Security in Mobile Devices (Draft). *NIST Special Publication*, *800*, 164.

ConstU.S.. art. IV (1787).

ConstU.S.. Pmbl(1787).

U.S. Const. amend. IV (1791).

Cyber-Intelligence Sharing and Protection Act, (2013). H.R. 3523, 112th Congress (2011-2012), (2012), H.R. 624,113th Congress (2013-2014)

Cybersecurity. (2014). Retrieved June 14, 2014 from http://www.phe.gov/Preparedness/planning/cip/Pages/eo13636.aspx

Cybersecurity Act of 2012, (2012). S. 2105, 112th Congress (2011-2012).

Cybersecurity bill wins key Senate vote, upi.com. (2012). Retrieved June 14, 2014 from http://www.upi.com/Top_News/US/2012/07/26/Cybersecurity-bill-wins-key-Senate-vote/UPI-57801343345113/

Cybersecurity Framework. (2014). Retrieved June 14, 2014 from http://www.dhs.gov/publication/eo-13636-improving-ci-cybersecurity

Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). The Future of National and International Security on the Internet. In A. Kayem & C. Meinel (Eds.), *Information Security in Diverse Computing Environments* (pp. 149–178). Hershey, PA: Information Science Reference; doi:10.4018/978-1-4666-6158-5.ch009

Department of Health and Human Services. (2014). *HHS Activities to Enhance.* Author.

Department of Homeland Security. (2014). *Section 10(a) and 10(b) Report on the United States Coast Guard (USCG) and Maritime Critical Infrastructure Cybersecurity Standards,Section 10(b) Report on the Department of Homeland Security's Chemical Facility Anti-Terrorism Standards (CFATS)Section 10(b) Report on the Transportation Security Administration's (TSA's) Approach to Voluntary Industry Adoption of the NIST.* Author.

Egan, M. (2014). *Judge Rules FTC Can Sue Wyndham Over Cyber Security Lapses.* Retrieved June 16, 2014 from http://www.foxbusiness.com/industries/2014/04/08/us-ftc-can-sue-hotel-group-over-poor-data-security-court-rules/

Electronic Communications Privacy Act of 1986, (1988). 18 U.S.C. §§ 2510-2511

Exec. Order No. 13636, (2013). 78 FR 11737, 11737 -11744

Federal Trade Commission Act, (1914). 15 USC §§ 41-58

FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information. (2014). Retrieved June 16, 2014 from http://www.ftc.gov/news-events/press-releases/2011/03/ftc-accepts-final-settlement-twitter-failure-safeguard-personal

Gramm–Leach–Bliley Act of 1999, (2000). 15 U.S.C. §§ 6801-6809; 6821-6827

Harris, S., & Meyers, M. (2002). *CISSP*. McGraw-Hill/Osborne.

Health Insurance Portability and Accountability Act of 1996, (2000). 42 U.S.C. §§1320d-1320d-9

Health Insurance Portability and Accountability Act of 1996, Privacy and Security Rule, (2003). 45 C.F.R. §§ 164.102-164.534

Homeland Security Act of 2002, (2006). 6 U.S.C. §§ 101-613 Federal Information Security Management Act of 2002, (2006). 44 U.S.C. §§ 3541-3549

Janczewski, L., & Colarik, A. (2008). *Cyber Warfare and Cyber Terrorism*. Hershey, PA: IGI Global; doi:10.4018/978-1-59140-991-5

Jansen, W., & Karygiannis, A. T. (1999). *SP 800-19. Mobile Agent Security*. Gaithersburg, MD: National Institute of Standards & Technology.

Jansen, W., & Scarfone, K. (2008). Guidelines on cell phone and PDA security. *NIST Special Publication*, *800*, 124.

Lardinois, F. (2012), *U.S. House passes controversial CISPA cybersecurity bill 248 To 168.* Retrieved June 14, 2014 from http://techcrunch.com/2012/04/26/u-s-house-passes-cispa-248-to-168/

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic & International Studies.

Marbury v. Madison, (1803). 5 U.S. 137

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: security and privacy considerations. *It Professional, 14*(5), 53-55.

National Institute of Standards and Technology (NIST). (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. United States of America.

Notice of Breach of Security Act, (2003). Cal. Civ. Code § 1798.29

Sarker, S., & Wells, J. D. (2003). Understanding mobile handheld device use and adoption. *Communications of the ACM*, *46*(12), 35–40. doi:10.1145/953460.953484

State of California Department of Justice Office of the Attorney General. (2013). *Getting smart about smartphones, tips for parents.* Retrieved June 14, 2014 from http://oag.ca.gov/privacy/facts/online-privacy/smartphones-parents

The White House. (2014). *Assessing Cybersecurity Regulations*. Retrieved June 14, 2014 from http://m.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations

U.S. Const. art. I, § 8, cl. 1 (1787).

U.S. Const. art. I, § 8, cl. 3 (1787).

U.S. Const. art. III, §§ 1-2 (1787).

U.S. Environmental Protection Agency. (2014). *Section 10(b) report on the environmental protection agency's water and wastewater critical infrastructure cyber-security preparedness.* Retrieved June 14, 2014 from http://water.epa.gov/infrastructure/watersecurity/upload/EO_13696_10-b-_EPA_response.pdf

Welch, D., & Lathrop, S. (2003, June). Wireless security threat taxonomy. In *Information Assurance Workshop* (pp. 76-83). IEEE.

KEY TERMS AND DEFINITIONS

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (Harris, 2002).

Availability: Timely, reliable access to data and information services for authorized users (Harris, 2002).

Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices (Harris, 2002).

Cyber Terrorism: Attacks with the use of the Internet for terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses, worms, Trojans, and zombies (Janczewski & Colarik, 2008).

Device Owner: Entity that has purchased and maintains ownership of device (Chen et al, 2012).

Information Owner: An application-specific provider, a digital product provider, or an enterprise that allows access to resources from mobile devices, (Chen et al, 2012).

Integrity: Quality of an IS reflecting the logical correctness and reliability of the OS; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (Harris, 2002).

Mobile Device: This device type is usually referred to as a handheld, handheld device or handheld computer (Sarker & Wells, 2003).

Non-Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (Harris, 2002).