Spring 2013
Industry Study

Final Report
Information and Communications Technology (ICT)

The Dwight D. Eisenhower School for National Security and Resource Strategy
National Defense University
Fort McNair, Washington, D.C. 20319-5062

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) 2013

ABSTRACT: The Dwight D. Eisenhower School for National Security and Resource Strategy's 2013 Information and Communication Technology (ICT) Industry Study seminar analyzed the health of the ICT industry. The seminar concluded that the ICT Industry is thriving, but vulnerabilities exist that could threaten the U.S. national security and its economic competitive advantage as an industry leader. They gained insight into the current condition of the ICT industry, including technology trends that are causing significant shifts in business strategy, an overview of the U.S government's role in the knowledge economy, and potential industry vulnerabilities. The seminar further concludes that, as economic prosperity becomes increasingly dependent on the ICT industry, the government will be challenged to maintain the tenuous balance between free market operations that encourage innovation, economic growth, and prosperity, and national security strategy, policy, and budgets.

Lt Col Reginald Ash III, U.S. Air Force
LTC Abdellah Athmani, Moroccan Army
CDR Kevin Austin, U.S. Navy
CAPT Luiz Basso, Brazilian Navy
Mr. William Corbett, Department of Justice
CAPT Sonya Ebright, U.S. Navy
Lt Col Frank Flores, U.S. Air Force
COL Mary Foreman, U.S. Army
Lt Col Glen Genove, U.S. Air Force
COL Greg Jicha, U.S. Army
CDR Matthew Kosnar, U.S. Navy
Mrs. Julia Lyons, Department of the Army
LtCol Michael McWilliams, U.S. Marine Corps
Mr. Michael Shanahan, Department of Justice
Ms. Jeanine Smith, U.S. Coast Guard
COL Patrick Walsh, U.S. Army
COL Sidney Zemp, U.S. Army

Mr. Feza Koprucu, Department of Homeland Security, Faculty Lead
COL Richard Altieri, J.D., U.S. Army (Retired), Faculty
COL David King, Canadian Forces (Retired), Faculty
Col Lynne Thompson, EdD, U.S. Air Force (Retired), Faculty

PLACES VISITED

Domestic:
Apple Inc. (Cupertino, CA)
AT&T Inc. (Washington, DC)
BlackBerry (Irving, TX)
Brocade Communications Systems, Inc. (San Jose, CA)
Cisco Systems, Inc. (San Jose, CA)
Computer Sciences Corporation (Falls Church, VA)
Congressional Research Service (Washington, DC)
CTIA - The Wireless Association (Washington, DC)
Defense Information Systems Agency (Ft. Meade, MD)
Department of Homeland Security (Arlington, VA)
EMC Corporation (Santa Clara, CA)
Ericsson (Plano, TX)
Facebook, Inc. (Menlo Park, CA)
Google Inc. (Mountain View, CA)
Huawei Technologies Co. Ltd (Plano, TX)
Information Technology and Innovation Foundation (ITIF) (Washington, DC)
International Business Machines Corporation (IBM) (Federal) (Washington, DC)
Microsoft Corporation (Reston, VA)
Software and Information Industry Association (SIIA) (Washington, DC)
Sprint Nextel Corporation (Reston, VA)
TechAmerica (Washington, DC)
Telecommunications Industry Association (TIA) (Washington, DC)
Twitter (San Francisco, CA)
U.S. Cyber Command (Ft. Meade, MD)
Verizon Communications Inc. (Ashburn, VA)

International:
None

1. INTRODUCTION

The rapid globalization of information and communications technology (ICT) is providing the world's population with unprecedented access to information.[1] As explained in *The Human Face of Big Data*, "Today, a street fruit stall in Mumbai can access more information, maps, statistics, academic papers, price trends, futures markets, and data than a U.S. president could a few decades ago."[2] Connectivity does more than give people access to information; every connection—whether through a computer, phone, or GPS-enabled device—produces data. As Google Chief Executive Officer, Eric Schmidt noted, "From the dawn of civilization until 2003, humankind generated five exabytes of data. Now we produce five exabytes every two days… and the pace is accelerating."

As businesses and governments capitalize on the rising flow and availability of data, economic competition is increasingly dependent on the creation and assimilation of knowledge. In essence, the global economy is transforming from one that is "based on natural resources and physical inputs to one based on intellectual assets."[3] Our economy is now a knowledge economy and the ICT industry is at the heart of it. Every sector of the economy—finances, healthcare, critical infrastructure, and more—is leveraging ICT to increase productivity and speed the delivery of services and capital. As such, ICT is now an essential component in the routine functioning of the nation's critical infrastructure.

In a world where virtually every sector of the economy is inextricably linked to ICT, vulnerabilities that threaten the strength of the ICT industry also jeopardize national security. The nation's substantial dependence on the integrity and availability of ICT led President Obama to declare that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cyber security."[4] Since ICT cannot be separated from either economic welfare or national security, the United States (U.S.) government must strike a balance between securing the nation and fostering industry growth, progress, and innovation

For the past five months we have studied the domestic and global ICT industry in the evolving knowledge economy. Through our visits with ICT trade associations, business executives, and government leaders in the Washington, D.C., Silicon Valley, and Dallas/Fort Worth areas as well as extensive research of current industry literature, we determined that while the industry is thriving, vulnerabilities exist that could threaten U.S. national security and its competitive advantage as an ICT industry leader. With U.S. government buying power in the ICT industry waning and policymakers struggling to keep pace with the interminable footrace of technological progress, it is clear that to best facilitate continued U.S. development and global leadership, the U.S. government must partner effectively with industry.

In this report, we provide insight into the current condition of the ICT industry, including technology trends that are causing significant shifts in ICT business strategy, an overview of the U.S government's role in the knowledge economy, and potential industry vulnerabilities. We conclude the report with policy considerations for the U.S. government. As economic prosperity becomes increasingly dependent on the ICT industry, the government will be challenged to maintain the tenuous balance between free market operations that encourage innovation, economic growth, and prosperity, and national security strategies, policies, and budgets.

2. ICT INDUSTRY IN THE KNOWLEDGE ECONOMY

2.1. Health of the Industry

In 2012, the ICT industry generated $1.2 trillion in revenue and $179.77 billion in profits.[5] That said, it is unwise to provide a sweeping generalization about the health of the ICT industry since the industry is comprised of fifteen extremely diverse segments. To provide a better assessment of the industry, we developed a framework that categorizes the fifteen different segments of the ICT industry based on their role in the knowledge economy (see Appendix A for a graphical depiction of this framework). The framework consists of four layers: (1) Analysis, (2) Processing, (3) Gateway, and (4) Transmission. The segments in layer one have the highest level of interaction with data in the knowledge economy while layer four has the lowest. The following provides a high-level overview of the health of the industry segments within each layer of the knowledge economy, including their current condition and outlook.

Layer 1: The Analysis Layer

Layer one is comprised of industry segments that develop software or provide services that analyze and present data. Additionally, industry segments in this layer often use or sell the data they capture and analyze. For example, in the search engine segment, companies analyze data captured from users and provide a service, such as targeted advertising, based on this analysis. The segments in this layer are: search engines, Internet publishing and broadcasting, software publishing, and information technology (IT) consulting.

The segments in this layer are extremely healthy. Made up of over 480,000 companies, this layer experienced combined profits in excess of $88.3 billion in 2012.[6] The five-year projected Industry Value Added (IVA) by segment ranges from 2.62 percent to 11.46 percent, with a 5.5 percent average.[7] This layer, which includes some of the most dynamic and innovative companies in the industry and overall U.S. economy, is expected to contribute to industry and overall economic growth for many years.

Layer 2: The Processing Layer

Layer two consists only of the data processing and hosting services segment, which includes companies that process, store, and host the data of the knowledge economy. The technology in this segment enables the data analysis that occurs in layer one. Made up of over 50,000 companies, this segment's combined profit exceeded $10.1 billion in 2012.[8] While this segment's five-year projected IVA (2.6 percent) is just above projected gross domestic product (GDP) growth during the same period (2.1 percent), this segment is undervalued.[9] Current ICT industry trends (discussed in section 2.2) are positioning this segment for higher growth.

Layer 3: The Gateway Layer

Layer three is comprised of industry segments that provide hardware components, primarily used by humans, to interact with the knowledge economy. These segments offer a gateway to the knowledge economy by providing the technology and computing power needed to interpret data from devices such as smartphones, tablets, personal computers, and high performance computers. The segments in this layer are: communication equipment manufacturing, computer peripheral manufacturing, and computer manufacturing.

As a whole, layer three is the weakest layer of the ICT industry in the knowledge economy. Comprised of over 1,400 companies, this layer's five-year projected IVA is low, ranging from

negative 2.16 percent to positive 3.76 percent, and its combined profit was just over $5 billion in 2012.[10] As a whole, U.S. ICT manufacturing is declining as competition from offshore manufacturers is driving down prices.[11] U.S. computer manufacturing has been hit particularly hard by the emergence of substitute products like tablets.[12] There could be an even more dramatic drop off in this segment if Intel's new processing chip (anticipated to arrive in the fall of 2013) proves successful. Requiring less power, with little to no processing speed degradation, the chip could dramatically increase tablet capability, further reducing demand for standard personal computers.[13] One area of growth in the otherwise declining industry segment of computer manufacturing is high-performance computing (HPC).[14] In one worldwide study, 97 percent of companies that had adopted HPC said they could no longer compete or survive without it.[15]

Layer 4: The Transmission Layer

Layer four is comprised of industry segments that transmit data across the knowledge economy. The business models of companies in this layer primarily focus on data transmission, not processing, production, hosting, capture, or analysis. In other words, businesses in this layer of the knowledge economy are not adding value to data as they transmit it. The segments in this layer are voice over Internet protocol (VoIP) providers, wireless telecommunications carriers, Internet service providers (ISPs), telecommunication resellers, wired telecommunications carriers, satellite telecommunications carriers, and telecommunication networking equipment manufacturing.

Made up of over 8,000 companies, the segments in layer four experienced combined profits in excess of $76 billion in 2012.[16] The layer's five-year projected IVA ranges from negative 2.58 percent to positive 10.98 percent.[17] As a whole, the segments in this layer are stable. The three segments expected to experience the most growth are: VoIP, wireless telecommunications carriers, and ISPs.[18] The one declining segment is telecommunication networking equipment manufacturing.[19] Like in other ICT manufacturing segments, the number of U.S. companies in this segment is declining as imports are increasingly being relied on to satisfy domestic demand.[20] This segment is unhealthy and its projected IVA is likely to decline over the next five years.[21]

2.2. Industry Trends

The health of the ICT industry and the strategies of companies in it are heavily influenced by technology trends. Throughout the seminar's research, five technology trends were continuously identified as driving change in the industry:

- ***Cloud computing***: Cloud computing refers to the paradigm whereby data is stored, processed, and accessed across a network of Internet-accessible computers. This technology enables mass data storage and processing to be accomplished in ways never before envisioned. By shifting workload from local computers to a network of computers, which create a virtual "cloud," this new form of computing gives users access to data and applications on the Internet.[22] As IBISWorld notes, "IBM estimates that by 2015, cloud computing will overtake on-premise computing as the primary way organizations access information."[23] Virtualization of data centers, whereby software defined servers replace physical servers, is allowing greater computing capacities and efficiencies.
- ***Mobility***: While mobility is not a new trend, the "shift in consumer demand toward wireless products that offer the same functionality as wired products without the constraint of a fixed location" is continuing to transform the ICT industry.[24] Smartphones and, more recently, tablets have expanded the capability of mobile device computing while 4G network speeds are encouraging many users to completely abandon landlines.[25]

- ***Ubiquitous computing***: Leveraging capabilities provided by mobility and cloud, ubiquitous computing allows technology to "recede into the background of our lives" as everything that can benefit from connectivity is directly enabled with Internet Protocol capabilities.[26] As such, ubiquitous computing is often referred to as the "internet of everything" or "everyware."[27] One of the most prominent examples of ubiquitous computing is the Google Glass system that incorporates a camera, GPS, and all the functionality of Google's search engine into a futuristic-looking pair of wearable glasses.[28]
- ***Social networking platforms:*** Social networking platforms are web-based services that allow people to digitally connect with others.[29] Externally these tools can be used for business marketing, delivery, and intelligence. Internally they can be harnessed for sharing information, building relationships, and collaboration.
- ***Big data:*** This trend capitalizes on the vast amount of data—both structured and unstructured (i.e. videos, images, music, and documents)—the world is generating, transmitting, and collecting digitally. It uses powerful algorithms, software applications, and computing capability—often enabled by in-memory processing—to "find the hidden pattern, the unexpected correlation, [or] the surprising connection" in mass amounts of data.[30]

A Closer Look at Big Data

Big Data references can be found on almost every ICT industry website and in any web journal discussing the economy or innovation. Despite the buzz, the lexicon of big data is still being shaped and the term "big data" itself has subtle differences in meaning to different users. However, included in every nuance of definition is the notion of analyzing huge data sets. As the trade association TechAmerica explains, "Big data is not a technology, but rather a phenomenon resulting from the vast amount of raw information generated across society, and collected by commercial and government organizations. This phenomenon represents both a challenge in harnessing this volume of data, and an opportunity for government agencies who seek to enhance their effectiveness."[31] Though data and data analysis have been around for years, innovations in cloud computing, HPC, software development, data mining, and data storage have released a flurry of new innovations in big data.

IBM indicates that, "Fifteen percent of today's information is structured information that is easily stored in relational databases or spreadsheets. Unstructured information, such as email messages, videos, blogs, call center conversations, and social media posts, makes up about 85 percent of data generated today and presents challenges in deriving meaning with conventional business intelligence tools."[32] TechAmerica goes on to explore big data stating, "Information-producing devices, such as sensors, tablets, and mobile phones continue to multiply. Social networking is also growing at an accelerated pace as the world becomes more connected. Such information sharing platforms represent a fundamental shift in the way people, government, and businesses interact with each other."[33] While some companies refer to the explosion of data as big data, others refer to it as data mining, analytics, or predictive analytics when used to estimate new behavior.

According to *Wired.com*, "A customer-focused business with big data in its grasp has an unparalleled source of knowledge from an increasing number of sources now; mobile data, social data, transactional data, locational data, financial data, family data, medical data, carbon footprint, and consumption data. We even have data about data in the form of log data."[34] For the government, as written in the *Big Data Research and Development Initiative*, "Big data is defined as datasets too large for typical database software tools to capture, store, manage, and analyze."[35]

Experts estimate that in 2013, 3.6 zettabytes of data will be created, and that amount will double every two years. A zettabyte is equal to 1 billion terabytes, and a terabyte is equal to 1 trillion bytes.[36]

There is vast potential for big data in industry and government. Big data can improve, support, or even replace human decision-making.[37] It can optimize performance by enabling experimentation; reducing inefficiencies; eliminating waste, fraud, and abuse; and improving transparency.[38] The predictive capabilities of big data can improve mission outcomes and reduce security threats and crime.[39]

Success stories of big data analytics leading to higher profits have firms across industries excited, however, many are struggling to translate massive quantities of data into something useful. The need for specialization in big data problems and solutions has not only created a market for historical and real time data use, but has also created a new market for predictive analytics.

Big data has the potential to transform government and society but companies must first figure out how to effectively use it. Data, whether structured, unstructured, streaming, static, or relational, comes from a myriad of disconnected sources. Advanced algorithms, software applications, data storage receptacles, and HPC devices must be built to talk to each other to achieve new insights or solve problems. Across the world, software developers and data scientists are innovating, researching, and solving these problems. The breakthroughs and case studies of big data success stories have companies, universities, and governments investing huge sums of money to create new ways of harnessing data.

- Captain Sonya Ebright, U.S. Navy

Many companies in the ICT industry are experiencing varied financial performance as a result of these technology trends. While some are adjusting their strategies to take advantage of new opportunities, others find themselves struggling to deal with a quickly changing industry. The following sections detail different approaches ICT companies are using to respond to industry changes.

Increased Emphasis on the Enterprise

Cloud computing and big data are increasing the demand for HPC capabilities, computer servers, data centers, and wired and wireless Internet connections at the enterprise level.[40] As a result, computer manufacturing, telecommunications, ISP, and telecommunication networking equipment companies are shifting attention away from consumer sales to the enterprise. With the mobile market approaching saturation, telecommunications carriers are also shifting focus from the consumer market to the enterprise market. Additionally, as businesses become increasingly concerned about network reliability, security, and continuity, demand for high-end, domestically manufactured telecommunication networking equipment is expected to increase.[41]

Consolidation

With the notable exception of the wireless telecommunications carrier segment, which the Department of Justice (DOJ) has prevented from merging further, consolidation is taking place throughout the ICT industry.[42] The two factors most often cited for consolidation are (1) a company's desire to obtain new innovations and (2) market saturation. With regard to the former, the search engine and software publishing segments are leading the use of acquisitions and mergers to obtain technology innovations.[43] In both segments, well-established companies are purchasing

small start-ups with novel technologies to increase and, in some cases, diversify product and service portfolios.[44] As for the latter, saturation of the mobile market and the declining use of wired telephony is driving consolidation amongst ISPs, satellite telecommunications providers, wired telecommunications providers, and telecommunications resellers.[45]

Price Competition

While demand for mobility is high, saturation in the consumer mobile market is driving down prices of end user devices (i.e. smartphones) and service plans. As a result, telecommunications companies and communication equipment manufacturers are increasingly opting to compete on price, which will likely commoditize end user devices and service plans for consumers. The previously mentioned shift in focus from consumers to enterprises reflects how telecommunications companies are already anticipating and preparing for this commoditization.

At the same time, cloud computing and the preference for mobile devices (i.e. tablets) is putting downward pressure on prices for desktop and laptop computers and their associated peripherals (i.e. external hard drives).[46] According to industry experts, "The rise of tablet computers, which are excluded from this industry, will continue to pose a significant competitive threat… Not only are tablets exclusively manufactured abroad, but they also perform similar functions as industry laptops, contributing to the decline of already anemic sales of domestically made computers."[47]

Changing Business Models

While cloud computing is driving down prices in some segments of the ICT industry, it is simultaneously causing other segments, such as software publishing, to adjust their business models. The mobile app market is implementing "freemium," advertisement-based, transaction-based, and traditional paid sales models, while many of the legacy software publishing companies, including Microsoft and Adobe, are moving to subscription-based sales models to stabilize cash flows.[48]

Additionally, as mobile demand outpaces wireless spectrum availability, ISPs and telecommunications providers are expected to move toward usage-based pricing.[49] Usage-based pricing allows operators to capitalize on the exponential increase in data traffic that is occurring as a result of cloud computing, ubiquitous computing, social networking, and the demand for mobility.[50] Industry analysis suggests, "ISPs will start to charge users in proportion to the amount of data that they consume… Currently, about 5 percent of all ISP users account for 40 percent of network traffic, and industry operators view usage-based pricing as a more effective means of capitalizing on the increase[ing] in Internet traffic."[51]

2.3. Pervasiveness of ICT

ICT is generating wealth across the whole economy as companies employ technology to enable innovation and improve productivity. The ICT industry enables innovation by reducing design cycle time; lowering development, certification, and re-engineering costs; and improving performance and efficiency while reducing waste.[52] This improves return on investment (ROI) for the private sector and supports national security with sustained global economic competitive advantage. Viewed through a traditional market orientation, commercial innovation has long been understood as a function of research and development. Increasingly, however, its infusion has been running deeper into the entire value chain: investment strategy, intellectual property (IP), product engineering, manufacturing, marketing, sales, and distribution.

Today's data collection, enabled by ICT, supports the development of products and

services by providing the information needed for continuous refinement and incremental improvement. Additionally, other sectors of the economy are harnessing data mining, analytics, or predictive analytics to deliver new innovations. In many ways, innovation morphs conventional ROI, into "return on data."[53] Business models and jobs of tomorrow will increasingly involve harnessing, arraying and capitalizing on data, in what is often referred to as knowledge-based capital.[54]

The pervasiveness of ICT extends beyond industry into the personal lives of everyday citizens. As such, the knowledge economy is transforming elements of culture and society both at home and abroad.

In 1967, American psychologist, Stanley Miligram, conducted an experiment to form a picture of social connections in the United States. His findings became the now-famous "six degrees of separation" theory when his data proved that typically a trail of just six people bound society together.[55] In 2011, a group of 12 scientists replicated that famous experiment and found that with the aid social networking platforms; there are only "four degrees of separation" between us today.[56] The world has become increasingly interconnected, transforming the size of an individual's sphere of influence.

The National Intelligence Council's (NIC) *Global Trends 2025* predicted that increasing interconnectedness would enable individuals to coalesce in common cause and create new value networks. During the Arab Spring, the world witnessed how "social media [can] create an unstoppable cascade of change in politics and government."[57] This rising "power of the individual" stands to hold governments more accountable by forcing them to address social issues and deliver effective, transparent governance. Paralleling ICT's beneficial boost to the enfranchisement of marginalized populations, bad actors will also appropriate its innumerable advantages. As the NIC report observed, transnational networks will use advances in global communications to "recruit and train new members, proliferate radical ideologies, manage their finances, manipulate public opinion, and coordinate attacks."[58]

In addition to increasing interconnectedness and empowering individuals, ICT is morphing traditional concepts of privacy. Today's technologies collect our photos and comments, and information about our friends, hobbies, and interests in searchable databases available for scrutiny. The most minute private details of an individual's life are now recorded somewhere on the web. As Elizabeth Mason, an ICT industry analyst, stated:

> Privacy? What Privacy? And why not? People give up personal information in return for convenience. They hand over data about their Web activity for the chance to win a cruise. They let online game companies vacuum up personal tidbits from their Facebook accounts. Consumers share knowingly and unknowingly, through surveys, location-based services, searches, online resumes, photos, check boxes, check-ins, tweets, and clicks. People have no time to read gobbledygook privacy policies; they simply click 'I Agree.'[59]

3. U.S. GOVERNMENT IN THE KNOWLEDGE ECONOMY

The role of the U.S. government in the knowledge economy is threefold. The government (1) regulates and oversees the industry, (2) helps to secure both private and public sector ICT, and (3) applies ICT to the achievement of government missions.

3.1. Industry Regulation and Oversight

Through regulation of the ICT industry and the U.S. industry at large, the government creates conditions that can foster or, in some cases, unintentionally hinder ICT innovation and trade. One of the primary agencies responsible for regulating the ICT industry is the Federal Communications Commission (FCC), which "regulates interstate and international communications by radio, television, wire, satellite, and cable."[60] In addition, the ICT industry is subject to oversight from agencies that regulate and oversee the whole of U.S. industry (i.e. the Department of Commerce (DOC)) and enforce federal laws (i.e. the DOJ).

One of the most important ways that the U.S. government enables ICT industry productivity is through the development and protection of intellectual property (IP) laws.[61] Nationwide, the four industries with the highest level of patent intensity are segments of the ICT industry. According to the U.S. DOC, the country's most IP-intensive industries provide 40 million, or 27.7 percent, of all U.S. jobs.[62]

Industry regulation and oversight can also protect the rights of individual citizens. In this respect, the government is currently struggling to deal with the issue of privacy. With firms racing to gather data to predict consumer behavior and the government striving to prevent crimes and tax evasion, developing regulations to protect privacy is becoming more difficult, especially since regulation has the potential to inhibit company profits. Currently, there are over 40 laws in the U.S. that seek to protect an individual's privacy, but none are sufficient, "Data mining is so efficient that today's privacy protections are irrelevant. Once enough of your activities, however anonymous, are "datafied" a computer can identify you."[63] As technology has advanced, privacy protection has degraded to simply observing the problems, asking for self-regulation, and predicting dire consequences.

3.2. Security of ICT

The U.S. government's role regarding ICT security, particularly as it relates to private industry, is evolving. Within the government there are numerous agencies and departments with specific responsibilities and corresponding authorities for ICT security. The Department of Homeland Security (DHS) is responsible for protecting the government (".gov") domain and overseeing critical infrastructure, with the support of sector-specific regulatory agencies. The DOJ is responsible for cybersecurity law enforcement; the Department of Defense (DOD) is responsible for the defending the military (".mil") domain and conducting military operations; the National Security Agency (NSA) protects national security systems (NSS); and the U.S. intelligence community is responsible for cybersecurity intelligence. All federal agencies are responsible for adhering to Federal Information Security Management Act (FISMA) requirements, which are developed by the National Institute of Standards and Technology (NIST), as well as the NSS requirements, which are developed by the NSA. The Office of Management and Budget (OMB) ensures government agencies meet FISMA requirements. Finally, various agencies are involved in cybersecurity research and development. For more information about agency roles and responsibilities regarding ICT security, see Appendix B.

3.3. Application of ICT

Over the past decade, the federal government has spent $600 billion on IT to capitalize on opportunities presented by worldwide ICT advances.[64] From command and control of first responders via a single broadband network to predictive analytics forecasting societal trends, the U.S. government is leveraging ICT to achieve national security objectives, improve services for

its citizenry, and make more efficient use of taxpayer dollars. For specific examples of how the U.S. government leverages ICT in support of its missions, refer to Appendix C.

Procurement of federal IT is subject to governance established by the President, the OMB, the Federal Chief Information Officer (CIO), agency CIOs, and Congress (see Appendix D). Since 2009, the Obama administration has published multiple forms of IT guidance for federal agencies (see Appendix E). Most recently, the House Committee for Oversight and Government Reform passed the Federal Information Technology Acquisition Reform Act (H.R. 1232). The proposed legislation strengthens the role and authority of agency CIOs, codifies a number of the current administration's IT policies and the role of the Federal CIO, endorses the use of open source software, promotes increased use of "fixed price technical competition" or "bid to price" contracts, and establishes a "Federal Infrastructure and Common Application Collaboration Center" and a collection of agency-based "Assisted Acquisition Centers of Excellence."

4. POTENTIAL VULNERABILITIES

4.1. Cyber Security and Critical Infrastructure

Throughout most of American history, threats to national security fell squarely within the purview of government agencies. Cyber threats changed that paradigm, as the U.S. government can no longer effectively secure its assets without assistance from the private sector. Nearly 85 percent of U.S. critical infrastructure is owned by the private sector, including the ICT industry.[65] As a result, transmission of U.S. data and voice communications are practically guaranteed to traverse privately owned critical infrastructure. Increasingly, these critical infrastructures are experiencing cyberattacks that threaten to disrupt every aspect of our economy and society. Cyberattacks on financial institutions have resulted in lost funds and decreased confidence in the banking system. Cyber espionage attacks on military and private networks have resulted in the extensive loss of IP, which could allow our enemies to bypass generations of research and development and more rapidly create countermeasures to U.S. military weapon systems.

The U.S. Government Accountability Office (GAO) estimates that the number of organizations conducting cyberattacks against the U.S. has increased by a factor of nine over the past six years, from 5,500 in 2006, to 48,500 in 2012.[66] These organizations include criminal enterprises, "hacktivists," and nation states, of which 20 to 30 currently possess significant cyberwarfare capabilities.[67] Nation states with advanced cyberwarfare capabilities include the People's Republic of China (PRC), Russia, Iran, and North Korea, all of who are either competitors or self-proclaimed enemies of the U.S. On the other end of the spectrum, asymmetric cyber threats are posed by political activists, criminals, and aspiring hackers. Unlike any other threat to national security, cyberattacks from a single actor, thousands of miles, away can inflict disproportionate damage to the U.S.

Nefarious cyber actors have the ability to affect U.S. national security through attacks on both military and commercial systems. In the energy sector alone, attacks on critical energy infrastructures increased 52 percent between 2011 and 2012.[68] The 2012 Norton Cybercrime Report showed that globally the loss due to cybercrime was $110 billion, with a cost to U.S. consumers of approximately $21 billion.[69] Banks, telecommunication companies, power grids, and just about any organization conducting research and development are at risk.

In some fashion, the ICT industry is arguably reliant upon most, if not all, of the 16 critical infrastructure sectors (CIS) defined by the DHS. However, the ICT industry's existence and effectiveness depend primarily on the health and availability of three particular CIS: communications, information technology, and energy. Any disruption of these sectors would have

an immediate and significant impact on the ICT industry as a whole. Conversely, the effectiveness of each of the 16 CIS is largely dependent on ICT industry services. Without computers or telephones, no infrastructure sector within the U.S. would function properly. For example, the emergency services sector would be severely crippled if a disruption to the communications sector prevented the use of 911 emergency services. In short, the ICT industry has a symbiotic relationship with each of the 16 CIS. All are dependent on each other for maximum utility and future growth.

The past three administrations have increasingly focused on cybersecurity, primarily through Presidential Directives and Executive Orders mandating departments and agencies of the executive branch share information to the greatest extent possible amongst themselves and with private industry. What remains lacking is comprehensive cybersecurity legislation. One step towards rectifying this shortcoming is the currently proposed Cyber Intelligence Sharing and Protection Act (CISPA). The stated goal of this legislation is to help the U.S government investigate cyber threats and ensure the security of networks against cyberattacks, primarily through sharing Internet traffic information between government agencies and "private-sector entities and utilities" with regard to internet traffic information.[70] While CISPA's future remains uncertain, due in large part to privacy concerns, it is a step in the right direction. Until appropriate legislation is implemented, individual companies must continue to develop their own plans to monitor and protect their systems from intrusion.

The U.S. government is clearly designated responsible for the security of military and government cyber systems (".mil" and ".gov" domains). However, there is no single organization responsible for providing that same level of protection to the commercial (".com") domain, where the ICT industry, including the communications and information technology CIS, operate extensively. While strides have been made in protecting the commercial domain, the Internet remains a vulnerable pathway for malicious actors to wreak havoc on an immense scale. Working together, the government and private sector can continue to identify and mitigate these threats.

Cybersecurity and the Advanced Persistent Threat

It is nearly impossible to open a newspaper, surf the Internet, or watch the evening news today without encountering a warning of the omnipresent danger of cybercrime. In 2012, Americans lost approximately $21 billion as a result of nefarious cyber activity including monetary theft, identity theft, and fraud.[71] Considering nearly two thirds of adults online worldwide have been victimized by cybercrime, it is easy to understand and appreciate the economic impact of such criminal activity.[72] Unfortunately, these statistics do not convey the full scope of cybercrime's negative effect on our country.

A far more insidious type of cybercrime, known as "Advanced Persistent Threats" (APT), is stealthily siphoning off extraordinary amounts of our most sensitive data and transferring it abroad.[73] APT groups are typically nation state-sponsored hacking teams dedicated to surreptitiously collecting intelligence rather than amassing financial gain.[74] For years, U.S. businesses and media have accused foreign countries, primarily the PRC, of conducting such intelligence collection efforts. However, as a result of the inherently anonymous nature of the Internet, accusations of cyber espionage have historically been met with defensive rebuttals rooted in plausible deniability. In February 2013, cybersecurity firm Mandiant altered the APT landscape by releasing a report identifying People's Liberation Army (PLA) Unit 61398 as the hacking group "APT1," which is responsible for conducting extensive cyber espionage attacks against the U.S. since 2004.[75]

Mandiant developed its assessment by conducting computer intrusion investigations at 141 U.S. victim companies over a period of seven years.[76] Analysis revealed patterns in APT1's tools, tactics, and procedures that strongly suggest a unified, coordinated effort to steal "broad categories of intellectual property" from U.S. organizations.[77] For example, between January 2011 and January 2013, 98.2 percent of the unique IP addresses used to access APT1's exploitation infrastructure resolved to just 4 net blocks in Shanghai, China—two of which were registered to the Pudong New Area where Unit 61398 is physically located.[78]

Based on investigative analysis, Mandiant concluded that Unit 61398 is likely staffed by hundreds, or potentially thousands of cyber operators.[79] The Unit maintains an elaborate infrastructure of computer systems around the world including 937 command and control (C2) severs hosted on 849 distinct Internet Protocol addresses in 13 different countries.[80] In addition, it employed custom malware and hacker tools to operate its infrastructure.

Since 2004, nearly every major U.S. industry has been targeted by Unit 61398's cyber espionage efforts, including the information technology, high-tech electronics, satellites and communications, and energy industries.[81] Once unauthorized access was obtained, APT1 remained undetected on its victims' networks for an average of 356 days.[82] As a result of Unit 61398's prolific abilities to surreptitiously penetrate and establish permanent footholds within target networks, Mandiant estimates that the PLA has exfiltrated hundreds of terabytes of data from the U.S. to China.[83]

The crown jewel in Mandiant's unveiling of APT1 was the identification of three individuals associated with the hacking group. Most significantly, Mandiant disclosed the identity of Wang Dong, a.k.a. "uglygorilla," a contributor to Unit 61398's computer network operations (CNO) since 2004.[84] China's ability to continually deny knowledge of, or participation in, cyber espionage will become increasingly difficult as more illicit activity is eventually linked to Chinese citizens. As Mandiant adeptly concluded, either Unit 61398 is APT1, or "a secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates."[85]

Mandiant took a calculated risk by disclosing Unit 61398's hacking activity. It is highly likely the PLA will now abandon its current infrastructure, alter its CNO techniques, reengineer its custom malware, and potentially relocate its physical office. All of these actions will make it more difficult for the U.S. intelligence community to track APT1 activities, and for our network operators to defend against new attacks. However, the decision to unveil Unit 61398 as the entity behind APT1 was a sound one. U.S. networks cannot be allowed to indefinitely hemorrhage sensitive data, and China must be confronted about its prolific embezzlement of our IP.

Fortunately, since the publication of Mandiant's report the demeanor of the White House and Pentagon regarding cyberespionage has changed. In May 2013, for the first time the Pentagon openly accused the PRC of using "computer network exploitation capability to support intelligence collection against the U.S."[86] The time has arrived for the U.S. to confront China about its cyberspying and aggressively seek to terminate it. Left unchecked, such blatant disregard for both American IP and international cyber norms will drive a wedge between the U.S. and the PRC, ultimately complicating our strategic national security rebalancing towards Asia. As an added benefit, successfully establishing cyber rules of engagement with China will provide a reusable framework for mitigating similar threats with other nation states.

- Michael Shanahan, U.S. Department of Justice

4.2. Intellectual Property

As mentioned previously, protecting IP is critical to innovation and the growth of the knowledge economy. Unfortunately, the threat of IP theft introduces risk to innovation and thus diminished economic rewards. The U.S. DOC estimates that the domestic value of stolen IP is between $200 billion and $250 billion annually. Such massive losses put the ICT industry and our economy at risk.[87]

The financial viability of many ICT companies is heavily dependent on ensuring confidentiality of sensitive IP; as a result, such companies are natural targets for attempted IP theft. IP theft can occur from both consumers and competitors. For years software manufacturers, such as Microsoft, have sought to prevent consumers from using a single software license on multiple computers. ICT companies also must protect their IP from competitors. For example, Apple is currently alleging in court that Samsung copied patented ideas and technology used in smartphones. Ironically, the founder of Apple, Steve Jobs, once said, "We have always been shameless about stealing great ideas."[88]

The Internet provides a medium for criminal enterprises, competitors, activist groups, and state-sponsored actors to steal IP. While these criminals frequently hack into networks to access IP, unsuspecting insiders who fall prey to phishing or social engineering attacks also unknowingly aid them.[89] A 2013 study by Symantec reveals that insiders are a serious threat to IP. This study identified that over half of corporate employees use risky data practices such as emailing business documents between work and personal accounts and using online file sharing applications without employer permission. These activities make the external criminal's job much easier. Equally concerning, more than half of employees take proprietary information with them when they leave a company.[90]

There is also a foreign policy aspect to IP theft. Annually, the U.S. Trade Representative (USTR) publishes a "Special 301 Report" on global enforcement of IP. The 2012 report listed 27 countries on a general "watch list," and 13 countries on a "priority watch list" for IP violations. The U.S. government takes bilateral actions with countries on these lists to improve foreign protection of U.S. IP.[91]

Domestically, a new U.S. business model threatens the value of IP in the ICT industry. In this business model, companies purchase patents from non-practicing entities, such as universities, with no intent to use the patent in manufacturing. These patent assertion entities (PAEs), known pejoratively as "patent trolls," create revenue by suing innovators and manufacturers for patent infringement. While PAEs provide much needed revenue to research centers, such as universities, many of their lawsuits are frivolous and cost the ICT industry billions of dollars annually. For example, PAEs cost the ICT industry $29 billion in 2009. Due to exorbitant court costs associated with defending patent infringement suits, most cases settle early in the process. When cases do proceed to a judgment, 92 percent of the time the PAE loses. In 2012, 61 percent of all infringement cases were filed by PAEs, and the rate is growing fast, increasing by 38 percent since 2007. These cases have an especially damaging effect on start-up companies that do not have the resources to defend themselves.[92]

U.S. companies and the U.S. government pursue multiple avenues to protect IP. Appendix F provides more information about steps companies are taking to protect IP while the upcoming section on policy considerations (section 5) addresses actions that can be taken by the U.S. government.

4.3. ICT Supply Chain

The ICT supply chain is an extremely complicated and diverse machine that links agencies, businesses, people, services, and products across ICT product life cycles throughout the world. The global nature of this supply chain, especially given that much of its manufacturing capability resides outside of the U.S., introduces numerous challenges that must be addressed by our policy makers. The NIST observed that the ICT supply chain "…is considered at 'risk' because of both the increased sophistication of information and communications technologies and the growing speed and scale of a complex, distributed supply chain."[93] Primary elements of risk in the ICT supply chain include export control, counterfeit proliferation, cyber espionage, and international suppliers.

With the increasing use of ICT in both commercial and military systems, export control is a growing concern to domestic ICT businesses that compete globally as regulations (even under President Obama's current export control reform initiative) have historically been unable to keep up with the pace of technological advancement. To reduce production costs, many businesses have implemented global supply chains that use lower tier manufacturers in foreign countries with less restrictive export controls.

With this trend has come the threat of counterfeit or maliciously altered components, such as integrated circuits (IC), which could have crippling effects on national security. As IC fabrication continues to move offshore, the ability to maintain trusted foundries is challenged. As such, a holistic national approach is needed if the domestic ICT industry is to continue to play a role in meeting future national security requirements.

While the administration is struggling to ease restrictions on items that, in many instances, have become commodity technology exports, it is also dealing with an equally threatening problem—controlling the import of counterfeit IC into the ICT supply chain. The Semiconductor Industry Association estimates that counterfeit components cost U.S. semiconductor companies more than $7.5 billion annually in lost revenue. Subsequent remediation to eradicate counterfeit components can be equally costly.[94]

In September 2010, the Missile Defense Agency learned that mission computers for the Terminal High Altitude Area Defense system contained suspected counterfeit memory devices. The primary contractor ultimately bore the $2.7 million in remediation costs.[95] In 2011, legislation was included in Section 818 of the National Defense Authorization Act for fiscal year 2012, placing the burden squarely on defense contractors to establish policies and procedures to eliminate counterfeit electronics from systems manufactured under DOD contracts.[96]

Supply chain vulnerabilities in the ICT industry have a high potential for large scale and long-term damage, as U.S. reliance on foreign IC suppliers creates "opportunities for adversaries to clandestinely manipulate technology used in critical microelectronics applications."[97] These opportunities provide "close access to a target technology throughout its lifetime, not just at inception."[98] In 2008, the Federal Bureau of Investigation (FBI) confiscated $76 million worth of Cisco routers that would have provided a backdoor into U.S. government computer systems and networks. The routers were purchased from an authorized Cisco vendor who had purchased the routers from an untrustworthy Chinese supplier.[99] Unfortunately, current export controls, combined with favorable overseas tax treatment, have effectively pushed the IC industry offshore. This trend increasingly undermines domestic foundries' ability to compete both in manufacturing and research and development.[100]

The international nature of the ICT supply chain lends itself to numerous vulnerabilities. Competition in the memory chip market has eliminated weaker manufacturers and left an oligopoly

that is beginning to act monopolistically. Today, four out of six memory chip manufacturers reside outside of the U.S.[101] A recent *Financial Times* article indicated that key manufacturers are reducing capacity expansion.[102] This reduction will take place during a period when smart phone demand is growing, resulting in higher component prices that have to be absorbed by the ICT industry and, ultimately, its customers. Additionally, reduced or metered production makes counterfeit operations more lucrative. When supplies start shrinking or authentic parts become more expensive, counterfeit markets thrive.

As an example, South Korea has become integral to the ICT industry through its manufacturing of end-user products, such as smart phones and tablets, as well as critical components, such as dynamic random access memory (DRAM). South Korean manufacturers account for two-thirds of global DRAM revenue today, and this is just one example of the country's significant contribution to the global ICT market. Bloomberg recently predicted that conflict on the tenuous Korean Peninsula would send shockwaves through the ICT world.[103]

4.4. Human Capital

The shift from a service-based economy to a knowledge-based one is increasing the demand for employees with strong science, technology, engineering, and mathematics (STEM) skills. While the total U.S. ICT labor market has remained slightly oversupplied for the last few years, demand from other sectors of the economy for ICT and STEM employees has the potential to create a labor shortage in the near future. Increasing the potential for this shortage are the nation's legacy educational system, poor labor mobility and labor pool utilization, and limits on H1B skilled labor.

With regard to the legacy educational system, U.S. universities have a poor track record bringing engineering students to the finish line. Approximately 40 percent of U.S. students who originally plan to achieve an engineering or science degree fail to stay in that program.[104] The American Universities Association identifies the legacy educational system as the problem. According to the association, university programs can modernize by offering more interactive classes, focusing on learning objectives (as opposed to conventional grading systems), and using project-based learning.[105]

Representatives from one telecommunications firm suggested that educational system problems extend beyond university programs. Many jobs in the ICT field require advanced math and computer training but not necessarily a college degree. Companies, however, have difficulty finding high school graduates with adequate math preparation. As such, firms are attempting to hire college graduates (who are presumably overqualified for these positions) while offering compensation that is often below what is offered for the same skillset in other business fields. The problem is that our K-12 system, to include vocational and technology magnet schools, are still largely tied to the legacy mindset of college preparation.

As for labor mobility, the ICT industry has a hard time placing workers with the right skills in the right place.[106] As previously mentioned, the total U.S. ICT labor market has remained slightly oversupplied for the last few years. According to the National Center for Education Statistics there were 152,950 graduates in IT-related programs in 2011, compared to 147,156 job openings (new jobs plus turnover) in 2012.[107] Despite excess supply, it is hard to satiate demand for ICT human capital in key ICT states like California, Virginia, Texas, and Washington. At the same time, several states with premier universities are producing surpluses of computer systems analysts, software developers, and database administrators.[108] Illinois and Pennsylvania have the biggest apparent surpluses of nearly 3,000 graduates, followed by Michigan, Indiana, Wisconsin, and Iowa.[109] In terms of labor pool utilization, both women and minorities, a potential source of

talent, are underrepresented in the ICT industry. While some firms are already pursuing these groups, many have failed to embrace any serious outreach and recruitment programs for women and minorities.

Finally, optimal supply in the ICT labor pool is only accomplished with a combination of both U.S.-born and foreign-born graduates of U.S. universities. As such, the current cap on H1B skilled labor presents an additional challenge for the ICT labor market. The current level for H1B skilled labor (bachelors) visas is 65,000 with an additional 20,000 for advanced (masters or above) visas. While the cap had been as high as 195,000, it slipped back to its default level of 65,000 when Congress failed to renew the increase in 2004.[110] Today the number of visas for specialized workers, are exhausted within months of being issued.[111]

An extremely difficult aspect of this analysis is quantifying the demand for ICT workers outside the ICT industry. As digital technology and connectivity pervades every aspect of our global economy, other sectors are seeking out ICT workers. Combined with outdated visa requirements that send educated workers out of the U.S. when their visas expire, it is easy to understand why our tech centers steadily bleed critical talent.[112]

4.5. Wireless Spectrum

Wireless communication is a core technology that greatly influences the growth of all economic sectors as well as our national security. The rising number of Internet accessible mobile devices has increased the volume of data traversing wireless networks. As data transmission loads escalate, the risk of congestion in the airways increases as well. Wireless broadband technology requires radio spectrum to function, and the quantity of spectrum currently allocated to wireless is not sufficient to handle projected demand growth.[113]

The lack of available wireless spectrum will impact national defense systems, emergency and communication systems, "Smartgrid" energy infrastructure, electric vehicle and intelligent transportation systems, advanced manufacturing systems, the financial industry, medical devices, and consumer electronics. Even with technological advancements allowing for more efficient use of existing spectrum, there still appears to be a shortage when considering projected usage increases. One way in which to realize the full potential of wireless broadband is to make new spectrum available to wireless services.[114] To accomplish this, spectrum that is currently underused or used in less valuable ways could be repurposed for use of wireless broadband.

The 2011 National Wireless Initiative (NWI) proposed doubling the amount of spectrum available for wireless broadband by 2021. NWI recommended reassigning 500 Megahertz of spectrum currently allocated for other uses, some of which would be repurposed from federal government uses, for wireless broadband. The National Telecommunications and Information Administration (NTIA) has been identifying portions of federal spectrum and shared federal and commercial spectrum that could be repurposed, in part by finding ways to make more efficient use of the remaining federal and shared spectrum.[115] In 2010, NTIA recommended that the U.S. government make available for wireless broadband115 Megahertz of spectrum currently used by federal agencies.

It should be mentioned that wireless providers could increase capacity without repurposing or innovating. Wireless providers can add more antennas or cell sites. Wireless companies are not pursuing this option, because it is not in the economic interest of the two largest wireless companies, AT&T and Verizon, who control the vast majority of wired connections to cell sites.[116] A wireless carrier providing services across a broad geographic area will have to buy some amount of wired connections from AT&T or Verizon, because they are the only provider in many locations. They control the supply of wired connections needed for additional cell sites and, by

keeping competitors' costs high for additional wired connections, create the perception of scarcity of wireless services. This is "characteristic anti-competitive oligopolistic behavior," which invites government action.

The wireless industry requested 800 MHz of additional spectrum, however, the FCC's National Broadband Plan, released in 2010, stated that there is little unallocated spectrum available. To solve the problem facing the U.S., a combination of the following must be pursued: sharing spectrum, repurposing spectrum to different bands enabled by efficient usage technologies, and increasing research on high-frequency usage.[117] As a result of the spectrum shortage, spectrum technology innovation has become a national priority.

4.6. Internet Governance

U.S. national security depends on a strong economy and the ability to protect strategic resources, of which the Internet is at the heart of both. The Internet connects over 2.2 billion people with over 500,000 new users coming online every day. The *Financial Times* estimates that the Internet economy will be worth $4.2 trillion by 2016, with annual growth rates of 8 to 18 percent in developing countries.[118] The nation's weapons, information, and energy systems, as well as its agriculture sector, are all increasingly dependent on the Internet. In the knowledge economy, the Internet is the global superhighway enabling organizations and consumers to conduct research, innovate, share ideas, and connect with others around the world.

Recently, global and national tensions regarding Internet governance have increased. The contest for control of the Internet has accelerated as technology has proliferated, and the Internet has become a critical infrastructure across global markets, and the defense and ICT industries. An initiative referred to as the "Internationalization of ICANN" (the Internet Corporation for Assigned Names and Numbers) could dramatically change Internet governance. The Internationalization of ICANN entails transferring the Internet governance functions from the U.S.-based ICANN to an international body, such as the United Nations' International Telecommunications Union (ITU). Members of the ITU presented a treaty proposal during the 2012 World Conference on International Telecommunications to expand jurisdiction that would give individual governments more control over the Internet. The treaty proposal, which could go into effect in January 2015, would allow pay-per-use tolls, heightened surveillance, and increased state control over the Internet. The U.S. has joined 54 other countries in refusing to sign the treaty, stating that it gives governments too much control over the Internet, and that it would harm Internet freedoms.[119]

Several U.S. ICT industry leaders have publically denounced the transfer of the Internet Assigned Numbers Authority (IANA) functions to the ITU and have stated that such a move would impair Internet stability and security. Industry leaders argue that the transfer would reduce the flow of free Internet traffic, resulting in unnecessary costs to industry and consumers. Vint Cerf, Google executive and one of the founders of the Internet, has gone on record stating that such a move would result in "creeping online censorship, higher costs for companies that use the Internet and the loss of the highly flexible technical arrangements that have enabled the global network-of-networks to thrive."[120]

At the national level, the "Open Internet" principle guides Internet governance. According to the FCC, "The 'Open Internet' is the Internet as we know it. It's open because it uses free, publicly available standards that anyone can access and build to, and it treats all traffic that flows across the network in roughly the same way… This openness promotes competition and enables investment and innovation."[121] The principle of Open Internet reflects the view that "consumers are entitled to certain rights and expectations with respect to their broadband service, including the right to: access the lawful Internet content of their choice; run applications and use services of their

choice, subject to the needs of law enforcement; connect their choice of legal devices that do not harm the network; and competition among network providers, application and service providers, and content providers."[122]

5. POLICY CONSIDERATIONS

Using U.S. national interests (articulated in the *National Security Strategy*) as a guidepost for the federal government's role in ICT policy, we offer ten policy considerations in three primary areas of interest: (1) protection of U.S. security; (2) development of a strong, innovative, and growing economy; and (3) respect for universal values.[123] In addition, the U.S. government must also develop policies to guide how it procures and uses ICT. Specific policy considerations for federal ICT procurement are included in Appendix G.

5.1. Protection of United States Security

- ***Strengthen the Cyber Security Legislation***: Many of the required cyber security structures for government-industry collaboration are either already in place or forming today. Recent cybersecurity mandates from the White House, such as Executive Order 13636 and Presidential Policy Directives 20 and 21, should be strengthened and codified in statute so that the U.S. government can continue to serve as an information clearinghouse on current and emerging threats and increase its ability to quickly share potentially classified or industry sensitive information.
- ***Secure Funding for the First Responders Network (FirstNet)***: This network holds tremendous promise to deliver revolutionary public safety and emergency data and voice services and solves the persistent problem of non-interoperable public safety communications systems. To enable deployment of FirstNet, the U.S. government should secure funding needed to deliver the most effective, resilient, and reliable network possible. We do not believe market incentives will be sufficient to expand the network; therefore, government involvement is appropriate.

5.2. Development of a Strong, Innovative, and Growing U.S. Economy

- ***Reduce Frivolous IP Lawsuits***: The DOC estimates that IP theft drains $200 billion to $250 billion from the U.S. economy each year. Greater Congressional attention in the IP arena is needed to better protect American businesses, innovators, jobs, and the country's economy. Additionally, Congress should act to reduce frivolous lawsuits from PAEs. Statutes should discourage frivolous lawsuits while maintaining a legal remedy for those whose IP was legitimately stolen.
- ***Direct Spectrum Sharing and Repurposing***: Wireless communication is a critical technology that influences economic growth, emergency communications systems, critical infrastructure, and U.S. national security. To minimize spectrum scarcity, the U.S. government should continue to identify available spectrum that can be reallocated for wireless use as well as federal spectrum that can be shared with the ICT industry.
- ***Reduce Export Control Reforms***: In light of previously discussed issues, the trusted foundry business is unprofitable for domestic IC firms and the DOD Trusted Foundry Program has been characterized as "putting a Band-Aid on a bullet hole."[5] The DOD and the IC need to jointly identify key sectors requiring protection to allow a more concerted focus on truly critical areas and their associated supply chains. Congress should enact tax and export reforms that address the drag current export laws exert on fast-moving technology sectors, while protecting technology that is too sensitive to share. Also, tax laws that discourage domestic IC

research and development, and push production offshore, require revision. Finally, members of Congress must prioritize national security demands over the needs of each member's respective constituents to protect critical sectors from market forces.

- ***Minimize Government Regulation of the Internet***: The principle of "Open Internet," which currently guides governance of the Internet at a national level, ensures that this vital economic resource continues to promote competition and enable innovation. As such, the U.S. government should maintain current policies supporting an open Internet based on market principles.
- ***Reform the Vocational System***: Jobs in wireless industry, data centers, and other ICT-related fields that do not require a college degree are competing for college graduates due to a dearth of high school graduates with adequate math preparation. To fill the gap, the U.S. government should consider reforms to the vocational high school system, including the creation of vocational training with solid mathematics preparation.
- ***Encourage Women and Minorities to Pursue STEM Careers***: Women and minorities are significantly underrepresented in the ICT industry. Some firms are already pursuing solutions to better balance their workforces, yet many others have failed to embrace serious outreach efforts to date. The U.S. government should consider developing K-12 and university level outreach programs to encourage female and minority students to pursue STEM studies.
- ***Increase the H1B Visa Cap***: Meeting the demand for ICT labor can only be accomplished with a combination of both U.S.-born and foreign-born graduates of U.S. universities. At the same time, the demand from the rest of the U.S. economy for knowledge workers is increasing. To avoid a talent shortage, the U.S. government should consider increasing the H1B cap for skilled labor and pursue reforms that will help retain critical skills in the U.S.

5.3. Respect for Universal Values

- ***Object to Excessive Government Control of the Internet***: As former Secretary of State Hilary Clinton noted, "Some governments use Internet governance issues as a cover for pushing an agenda that would justify restricting human rights online. We must be… united in our shared conviction that human rights apply online."[124] To protect the Internet's open architecture, user access, and freedom of expression, the U.S. should object to excessive government control over the Internet and support policies that foster free markets and global trade. More specifically, the U.S. should continue to manage IANA functions and participate within the international, multi-stakeholder Internet governance community.

6. CONCLUSION

In the interminable footrace of technological progress, three contestants (private industry, criminals, and individuals) have a distinct advantage over a third participant (government). The latter's headway is frequently constrained by deliberate, if not purposeful, impositions from institutions like Congress and the courts. Although designed to prevent official malfeasance, the burden of bureaucracy can often stifle growth rather than enable it. As one defense industry executive described it; government regulation is the epoxy that keeps the wheels of progress turning.

As ICT cannot be separated from either economic welfare or national security, it is imperative for the government to strike an advantageous set of stakeholder tradeoffs. Private actors, both lawful and malevolent, have become equally rapid, agile and asymmetric. In order to compete and thrive, U.S. firms rely on the U.S. government to keep pace. While balancing the

demands of security and privacy, the government must develop and manage channels that allow organizations to respond and adapt to continuously altering environments. In the process, the government must avoid hindering opportunities for U.S. firms to create and seize sustainable competitive advantage. This will require unprecedented transformation in many areas of the federal government. There really is no other alternative. As former General Electric CEO Jack Welch's cautionary assessment reminds us: "If the rate of change on the outside exceeds the rate of change on the inside, the end is near."

Today's ICT Advancements Shaping Tomorrow's Readiness

"The future is already here; it's just not very evenly distributed."

–William Gibson[125]

Could yesterday's computer science prodigies, the most forward thinkers of their time, ever have envisioned the technological revolution that their contributions helped launch? As Alan Turing deciphered the Enigma codes at Bletchley Park, and Grace Hopper programmed some 35,000 contacts across a span of three million connections and 500 miles of wire housed within IBM Mark-1's 51ft steel-framed box,[126] would they have dismissed notional descriptions of the computational power scaled into today's hand held devices as the creative musings of a Bradbury or an Asimov?

The future has a fantastical facet. Peering into it presents laymen, technologists and investors alike with a sort of proximity paradox. The further out in time one sets their predictive gaze, the more ambiguous the *terra incognito* of alternative futures appears to be. Uneasy with such obscurity and desirous of the familiar, stakeholders reflexively draw their focus onto the more circumstantial and immediate. This natural recess to reliable realms is embodied in the regular use of short-term, (typically 12-18 months) planning, purchasing, and funding cycles. However, when these inexorable futures finally *do* emerge, many private and public organizations find themselves woefully unprepared. The nearsightedness that informed such steady maneuvering during the short-term, leaves decision makers disoriented and ill-equipped to contend with the shockwaves of the long-term's precipitous arrival.

Even the histories of titans such as Microsoft, IBM and Apple contain epic encounters with missed cues that delivered near-fatal consequences. A firm's leadership can often conceive of critical changes inherent in the arriving future. However, the complexity of these changes often induce leaders to solidify those resource investments that delivered the firm to its current market position, rather than adjusting investments to facilitate successful adaptation to the oncoming changes.

In the last decade alone, ICT advancements have unfolded with unprecedented pace and penetration. They have shortened the arrival time of the long-term horizon and increased the cyclic rate of technological entry and obsolescence. And yet, the speed and depth of these advancements continue to transform the way we work, play, communicate and form relationships. As Thomas Friedman once reflected about 2004 –the year his book *The World is Flat* was first published– "Facebook didn't exist; Twitter was a sound; the cloud was in the sky; 4G was a parking place; LinkedIn was a prison; applications were what you sent to college; and Skype for most people was a typo."[127]Although these products and services have delivered incalculable benefits, understanding the full extent of their economic, political and cultural upheaval, within a legacy of expiring systems, remains a great challenge even in hindsight. Even Harvard Business School's Clayton Christensen, author of the seminal "disruptive technology" conception, has had

to continually update his theoretical framework to explain the impact of innovation's dizzying tempo on technology adoption, risk management and wealth creation.

If constructively responding to such systemic disruption is fundamental to the success of a firm or effectiveness of a government, then anticipating the pending upheaval in the first place becomes essential. Those organizations that recognize this strategic imperative will be more successful in devising coping strategies to harness the ensuing change and reap productive value from it. Those that do not will become wrenched between the discontinuities of knowledge and order, before being abruptly absorbed by Schumpeter's "creative destruction."

Propelled by the high-octane accelerant of innovation, tomorrow's ICT advancements will arise with even greater velocity. Novel combinations of cloud, mobile, sensor and virtual technologies will certainly continue to improve existing products and services, while other competitors race to design and deliver wholly new ones. This confluence of speed and inventive combining of technologies makes the challenge of prediction all the more difficult. As NASA Jet Propulsion Laboratory founder Theodore von Kármán observed when distinguishing the difference between science and engineering; the former seeks to understand *what is*, while the latter creates what *never was*.[128]

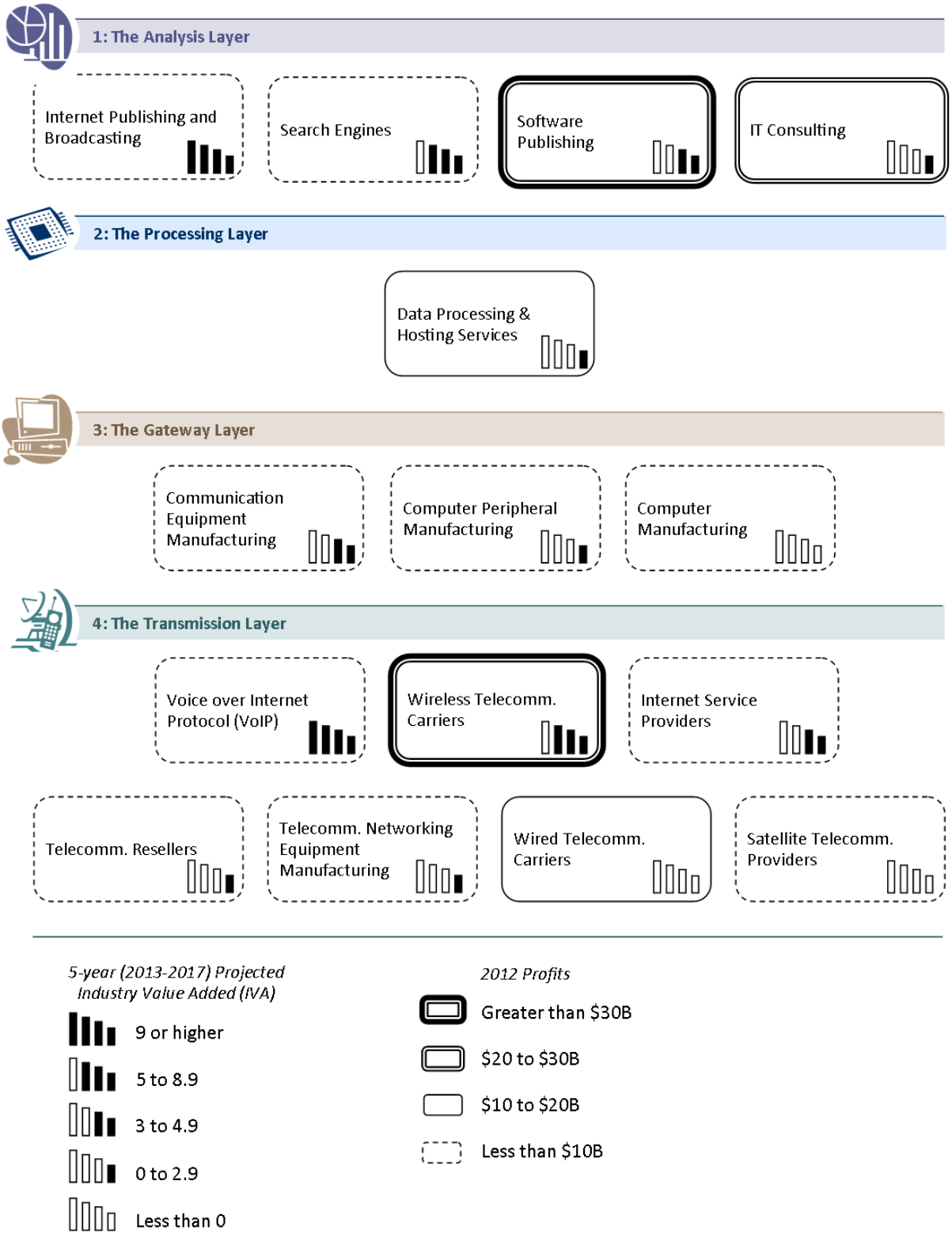
Today, new advances in 3-D printing, biomedical and nanotechnologies are moving from the frontiers of science to the front doorsteps of our homes and businesses. As the physical properties of the microchip approach their maximum functional capacity, science problems needed to open the doors to quantum computing are being solved sooner than originally expected. How all these discoveries integrate with existing structures, what they end up displacing, and who most successfully adapts to them, collectively stand to reshape much of our world. ICT will not only enable the development of these advancements, but will conjoin with them to generate things that "never were."

In a sense, this future environment will be as spellbinding to us, as today's would have been to the innovative computer pioneers of the 1940s. Technological speed requires an even greater concentration for developing a comprehensive approach to anticipate its impact. Speed without strategy is just lightening, not electricity. For the U.S. to preserve is dominant position in ICT, its firms and government will need to collaborate to shape that long term strategy.

- Mr. William Corbett, Department of Justice

The government's ICT policy posture must always maintain the tenuous balance between free market operations that encourage innovation and spark business success and regulations that provide security and protect privacy. This balance is difficult, especially in times of austerity, but maintaining balance, will enhance the health of the industry. The aforementioned policy recommendations drive the industry toward balance and sustainability, and contribute to the strength of America.

APPENDIX A: ICT INDUSTRY IN THE KNOWLEDGE ECONOMY (GRAPHIC)



APPENDIX B: FEDERAL AGENCY ROLES IN CYBERSECURITY

The Office of the White House Cybersecurity Coordinator, where the Coordinator is a member of President Obama's National Security Staff and also sits on the National Economic Council, highlights the link between cybersecurity and the economy.

The FBI Cyber Division focuses on preventing computer and network intrusions, identifying theft, and preventing online fraud. To accomplish its mission, the FBI works closely with industry and academia through the National Cyber Forensics and Training alliance (NCFTA), shares information through various industry-specific Information Sharing and Analysis Centers (ISACs), and maintains the Internet Crime Complaint Center (IC3) to "receive cyber crime related complaints from consumers and businesses for action by authorities, and to disseminate fraud alerts to the public."[129]

DHS' U.S. Computer Emergency Response Team (US-CERT), the operational arm of the National Cyber Security Division, "leads and coordinates efforts to improve cybersecurity posture, promote cyber information sharing, and manage cyber risks. It provides customer support and incident response, including 24-hour support in the National Cybersecurity and Communications Integration Center."[130] U.S. Immigration and Customs Enforcement (ICE) provides computer forensics support for both domestic and international criminal investigations, including benefits fraud, arms and strategic technology, money laundering, counterfeit pharmaceuticals, child pornography, and human trafficking involving the Internet. Finally, the U.S. Secret Service's (USSS) Financial Crimes Task Forces focus on the prevention of cyberattacks against U.S. financial payment systems and other critical infrastructure.[131]

APPENDIX C: U.S. GOVERNMENT APPLICATIONS OF ICT

C-1. First Responder Network (FirstNet)

In February 2012, Congress enacted The Middle Class Tax Relief and Job Creation Act of 2012, containing landmark provisions to create a much-needed nationwide interoperable broadband network that will help police, firefighters, emergency medical service professionals and other public safety officials execute their duties in a more safe and integrated manner. The governing entity responsible for the deployment and operation of this network—based on a single, national network architecture—is the new First Responder Network Authority (FirstNet), an independent authority within the National Telecommunications and Information Administration. FirstNet is charged with building, deploying, and operating the network, in consultation with federal, state, tribal and local public safety entities, and other key stakeholders.[132] All required spectrum licenses will be held by FirstNet.

The nationwide public safety broadband network holds tremendous promise to deliver revolutionary public safety and emergency data (and later voice) services. It solves the persistent problem of non-interoperable public safety communications systems. Elements required for the network to succeed include the following: (1) speedy network deployment and operational capacity; (2) leveraging the private sector's technologies, applications, and devices developed for commercial broadband; (3) a national emergency response center to ensure seamless communications between local, state, and federal governments; and (4) a dedicated funding stream to ensure this project remains financed at all levels of government.

This type of system will be useful during local, state, or federal emergencies such as the 9/11 terrorist attacks and Hurricanes Katrina and Sandy. The use of this system will dramatically enhance first responders' efforts to protect U.S. citizens, critical infrastructure, and ultimately national security.

C-2. The U.S. Department of Energy & Big Data

While the success of predictive analytics in crime prevention has been widely publicized, other segments of the government are also applying big data solutions in unconventional and phenomenal ways.

In support of the U.S. Department of Energy's (DOE) mission to "ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through transformative science and technology solutions,"[133] the DOE currently operates 17 national laboratories. Due to the highly sensitive and innovative work performed at these laboratories, securing the sites' physical, technological, and intellectual assets is crucial.[134] In an effort to better protect itself from potential threats, one of the DOE's laboratories contracted IBM to develop and implement a system to "detect, classify, locate and track potential threats—above and below ground—to secure its perimeters and border areas."[135]

Due to the physical size of the area to be secured, the DOE imposed several requirements on IBM during the system design phase. First, the solution was required to collect and analyze "massive amounts of digital acoustic data from biological, mechanical and environmental objects-in-motion."[136] To be effective, the system had to accurately differentiate among sounds from humans, animals, vehicles, and even the wind. Second, the expected volume of sensor data was so large, approximately 42 terabytes per day, that it could not be stored or analyzed at a later date.[137] Thus the system had to simultaneously record and analyze real-time input. Finally, the new system had to be interoperable with various types of sensors (i.e. audio, video, etc.), scalable to

accommodate perimeter changes, and extensible to ease integration with existing IT infrastructure.[138]

IBM partnered with TerraEchos to implement the TerraEchos Adelos S4 system, a covert security and surveillance solution that satisfied all of DOE's requirements. The Adelos S4 utilized advanced fiber-optic acoustic sensor technology licensed from the U.S. Navy. To process and analyze collected data, IBM implemented the InfoSphere Streams software from its big data platform.[139] InfoSphere Streams provided the ability to capture and process up to 1,024 streams of acoustic sensor data simultaneously. To put InfoSphere Stream's capabilities into layman's terms, this "would be akin to listening to 1,000 MP3 songs simultaneously and successfully discerning the word 'zero' from every song—within a fraction of a second."[140]

As a result of installing IBM's big data solution, including miles of fiber optic cable and thousands of sensors, the DOE laboratory was able to extend its security perimeter, save money, and ultimately gain a strategic advantage. In addition, by integrating both audio and video sensors, lab personnel are able to accurately detect and classify potential threats without accidentally identifying any false-positives.[141]

Using big data is extremely complicated and can be time consuming; however, if used correctly, its applications to law enforcement, critical infrastructure support, and other national security missions is limitless.

C-3. EINSTEIN Continuous Monitoring

To protect the U.S. government in the realm of cybersecurity the DHS has developed intrusion detection systems that utilize passive sensors to collect, analyze, and share information. One such system is the EINSTEIN Continuous Monitoring System, or EINSTEIN Program, which is an "automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government. By collecting information from participating Federal government agencies, the US-CERT builds and enhances our nation's cyber-related situational awareness. Awareness will facilitate identifying and responding to cyber threats and attacks, improve network security, increase the resiliency of critical, electronically delivered government services, and enhance the survivability of the Internet."[142]

The current version of the program, EINSTEIN 3, draws on "commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision-making on network traffic entering or leaving… Executive Branch networks."[143] While EINSTEIN's automated monitoring and response to potential threats before harm is done is a key element of its national security applicability, it monitors only U.S. government networks, leaving U.S. commercial entities and individual companies to develop their own plans to monitor and protect their systems from intrusion. No EINSTEIN equivalent currently exists to protect the Internet as a whole.

C-4. Joint Information Environment (JIE)

The DOD CIO strategic vision is to achieve an agile enterprise empowered by accessible, shared, and trusted information.[144] To codify and provide common vocabulary, in August 2012, the DOD CIO released the DOD Information Enterprise Architecture (IEA) 2.0. The DOD IEA 2.0 provides guidance for IT governance and the development of reference architectures.[145] the intent of DOD IEA 2.0 is to apply the lessons learned from conflict along with the emerging threats so that the services could achieve the Joint Information Environment (JIE). During our visit with the Defense Information Systems Agency (DISA), an executive described the JIE as "the stage

setter for C2 and decision support data access."[146] Its vision includes a data environment that is scalable, accessible, and that serves common interests.

As the threat of cyber attack increases, JIE is generally viewed favorably within the DOD, although skepticism and uncertainty continues to exist as the JIE shifts IT network control away from the services to an enterprise approach managed centrally by DOD. In addition, the services are still struggling with the concepts of cloud computing, defense enterprise mobility, ubiquitous computing, and big data, while the extension of the JIE to allied partners and defense industrial base contractors complicates matters further. [147]

APPENDIX D: FEDERAL IT GOVERNANCE IN THE EXECUTIVE BRANCH

There are four primary sources of IT governance within the executive branch of the federal government: the President, the OMB, the Federal CIO, and agency CIOs. At the highest level of the executive branch, the President establishes IT priorities and issues executive orders to manage operations of the federal government, including how it develops, manages, and applies IT. At the next level, the OMB manages the creation of the President's budget; develops information and IT policies; and oversees the effectiveness of federal agency IT programs, policies, and procedures. Residing within the OMB, the Federal CIO (sometimes referred to as the U.S. CIO) develops and provides direction on the use of IT in the federal government.

Within each federal agency, agency CIOs are responsible for establishing IT governance programs, policies, and procedures to ensure agency compliance with executive orders, OMB policies, and federal laws. Each agency CIO is a member of the Federal CIO Council. Chaired by the Deputy Director of Management, OMB, and directed by the Federal CIO, the council is responsible for improving federal IT management practices. The graphic below provides a high-level overview depiction of the executive branch IT governance structure.

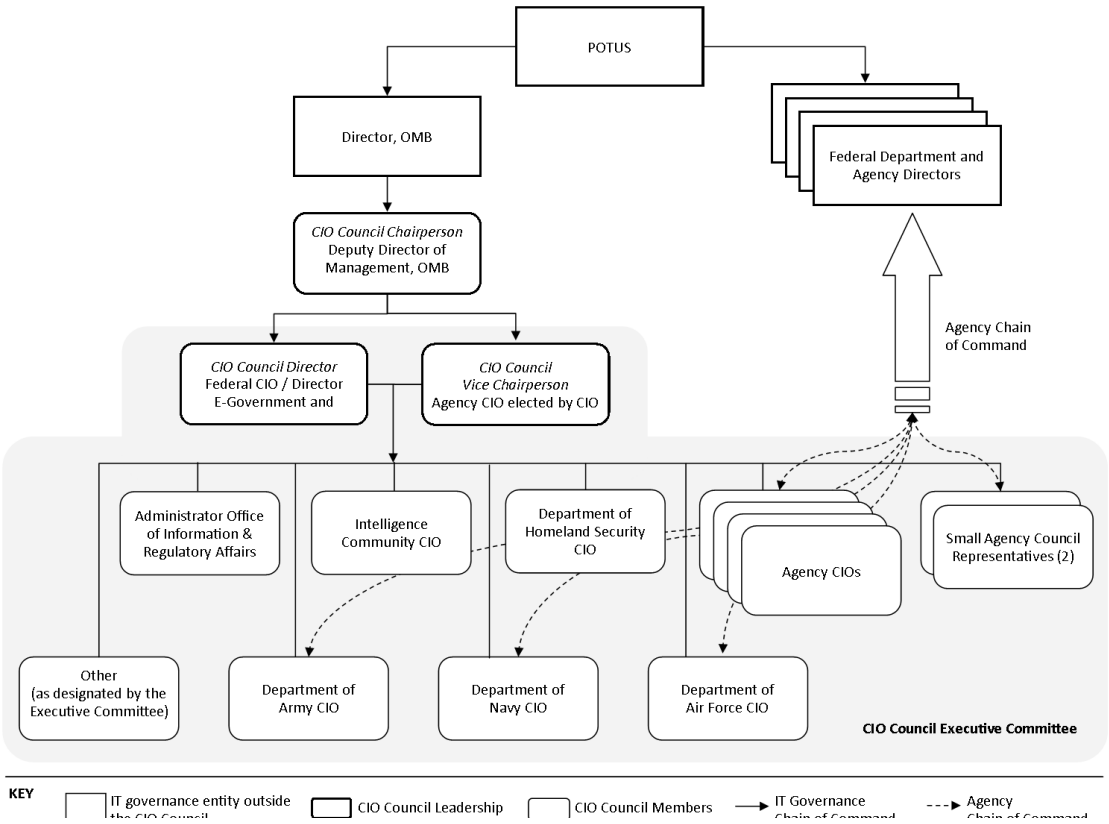


Figure 1. Federal IT Governance in the Executive Branch

APPENDIX E: THE OBAMA ADMINISTRATION'S FEDERAL IT POLICIES

Title	*Description*
Update on the Trusted Internet Connections (TIC) Initiative (OMB Memorandum M-09-32) (September 17, 2009)	Issued by the Federal CIO, this memorandum provides an update on the TIC initiative and requires agencies to update plans for implementing TIC requirements.[148]
Open Government Directive (OMB Memorandum M-10-06) (December 12, 2009)	This memorandum directs federal departments and agencies to implement the principles of transparency, participation, and collaboration set forth in the President's Memorandum on Transparency and Open Government, issued on January 21, 2009. Specific actions include publishing government data online, improving the quality of government data, institutionalizing a culture of open government, creating an Open Government policy framework, and developing an Open Government plan.[149]
Guidance for Online Use of Web Measurement and Customization Technologies (OMB Memorandum M-10-22) (June 25, 2010)	This memorandum, which supports the Open Government Directive, provides guidance on how agencies may measure website use without compromising the privacy of the American public.[150]
Guidance for Agency Use of Third-Party Websites and Applications (OMB Memorandum M-10-23) (June 25, 2010)	This memorandum, which supports the Open Government Directive, requires federal agencies to follow specific protocols when using third-party websites and applications to ensure privacy protection.[151]
Reforming the Federal Government's Efforts to Manage Information Technology Projects (OMB Memorandum M-10-25) (June 28, 2010)	This memorandum reiterates the administration's commitment to reforming management of federal IT and notifies agencies that the Federal CIO will conduct reviews of high-risk investments, prohibits agencies from awarding task orders on financial systems modernization projects, and notifies federal agencies of forthcoming recommendations from OMB's Deputy Director for Management on federal IT procurement and management practices.[152]
Immediate Review of Financial Systems IT Projects (OMB Memorandum M-10-26) (June 28, 2010)	Issued in concurrence with OMB Memorandum M-10-25, this memorandum "requires all CFO Act agencies to immediately halt the issuance of new task orders or new procurements for all financial system projects."[153]
Information Technology Investment Baseline Management Policy (OMB Memorandum M-10-27) (June 28, 2010)	This memorandum provides guidance for the development of agency IT investment baseline management policies, integrating requirements from OMB Circular A11, Federal Acquisition Regulation (FAR), and the Federal IT Dashboard.[154]
Immediate Review of Information Technology Projects (OMB Memorandum M-10-31) (July 28, 2010)	This memorandum, which supports OMB Memorandum M-10-25, initiates detailed reviews of high-risk IT projects and requires CIO Council agencies to identify high-risk IT projects, develop improvement plans for these projects, and present their plans in TechStat sessions.[155]
Evaluating Programs for Efficacy and Cost Efficiency (OMB Memorandum M-10-32) (July 29, 2010)	This memorandum provides information about how OMB is strengthening program evaluation for the 2011 budget process and requires agencies to submit "evidentiary support" for increased funding requests.[156]
Sharing Data While Protecting Privacy (OMB Memorandum M-11-02) (November 3, 2010)	This memorandum articulates the benefits of information sharing and reiterates that agencies must follow privacy requirements when sharing information.[157]

Title	*Description*
25 Point Implementation Plan to Reform Federal IT Management (25 Point Plan) (December 9, 2010)	Issued by the U.S. CIO, this document sets forth a plan for improving federal IT through the implementation of 25 action items. Action items are assigned with deadlines over an 18-month period to OMB, General Services Administration, the Federal CIO, Small Business Administration, CIO Council, Chief Financial Officer Council, and federal agencies. Most notably, the plan establishes the "Cloud First" policy and TechStat requirements.[158]
Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors (OMB Memorandum M-11-11) (February 3, 2011)	This memorandum continues the rollout of the HSPD-12 directive to enhance security and outlines a plan to expedite the use of federal personal identification verification credentials.[159]
Federal Cloud Computing Strategy (Cloud First Strategy) (February 8, 2011)	Issued by the U.S. CIO, this strategy provides a plan for implementing cloud computing as required by the "Cloud First" policy set forth in the 25 Point Plan.[160]
Streamlining Service Delivery and Improving Customer Service (Executive Order 13751) (April 27, 2011)	This order sets forth a requirement for agencies to develop customer service plans to improve user experience and streamline service delivery for both internal and external customers.[161]
Delivering an Efficient, Effective, and Accountable Government (Executive Order 13756) (June 13, 2011)	This order establishes a Government Accountability and Transparency Board to improve spending transparency; detect and remediate fraud, waste, and abuse; and improve government efficiency and speed.[162]
Implementing the Telework Enhancement Act of 2010: Security Guidelines (OMB Memorandum M-11-27) (July 15, 2011)	In support of the Telework Enhancement Act of 2010, this memorandum provides guidelines for adequately securing systems used for teleworking.[163]
Chief Information Officer Authorities (OMB Memorandum M-11-29) (August 8, 2011)	This memorandum broadens the role of agency CIOs from policymaking and infrastructure maintenance to IT portfolio management. It holds agency CIOs accountable for reducing costs, fixing or terminating troubled projects, and improving functionality more quickly.[164]
Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Executive Order13587) (October 7, 2011)	This order requires federal agencies and systems integrators to implement an "insider threat detection and prevention program" by the end of 2013.[165]
Promoting Efficient Spending (Executive Order 13589) (November 9, 2011)	This executive order reflects the administration's ongoing effort to ensure that the government is a good steward of taxpayer dollars. The order requires agencies to ensure that they are not paying for unused or underutilized IT devices and encourages implementation of agency-wide IT solutions.[166]

Title	*Description*
Implementing PortfolioStat (OMB Memorandum M-12-10) (March 30, 2012)	This memorandum establishes the requirement for agency CIOs, Chief Acquisition Officers, and Chief Financial Officers to participate in PortfolioStat reviews. A PortfolioStat is a "face-to-face, evidence based review… of an agency's IT portfolio."[167]
Federal Information Technology Shared Services Strategy (Shared-First Strategy) (May 2, 2012)	Issued by the U.S. CIO, this strategy "provides organizations in the executive branch… with policy guidance on the full range and lifecycle of intra- and interagency IT shared services… Commonly referred to as 'Shared-First,' this strategy requires agencies to use a shared approach to IT service delivery."[168]
Increasing Shared Approaches to Information Technology Services (OMB Memorandum) (May 2, 2012)	This memorandum introduces the Federal Information Technology Shared Services Strategy and sets forth an "Enterprise Roadmap" for agency CIOs. The memo requires the roadmap to be consistent with guidance provided in the 25 Point Plan, Cloud First Strategy, Digital Government Strategy, Common Approach, and Shared-First Strategy. The first roadmap was due August 2012 and agency CIOs must submit an updated roadmap annually (by 1 April).[169]
The Common Approach to Federal Enterprise Architecture (May 2, 2012)	Issued by OMB, this guide provides principles and standards for the development of business, information, and technology architectures and identifies how enterprise architecture integrates with strategic planning, capital planning, program management, human capital management, and cybersecurity.[170]
Digital Government Strategy (May 23, 2012)	Issued by the U.S. CIO this document sets forth a strategy to increase IT return on investment, reduce waste and duplication, and improve IT effectiveness.[171]
Improving Acquisition Through Strategic Sourcing (OMB Memorandum M-13-02) (December 5, 2012)	This memorandum establishes the Interagency Strategic Sourcing Leadership Council, which works in consultation with the CIO Council to "increase the use of government-wide management and sourcing of goods and services."[172] According to the memo, candidates for strategic sourcing include several IT commodities identified through the PortfolioStat process.[173]
Improving Financial Systems through Shared Services (OMB Memorandum) (March 25, 2012)	To improve modernization of financial systems, this memorandum "directs all executive agencies to use, with limited exceptions, a shared service solution for future modernizations of core accounting or mixed systems."[174]
Fiscal year 2013: PortfolioStat Guidance: Strengthening IT Portfolio Management (OMB Memorandum M-13-09) (March 27, 2012)	This memorandum provides guidance for fiscal year (FY) 2013 PortfolioStat reviews that builds on lessons learned from FY 2012 PortfolioStat reviews.[175]

APPENDIX F: INDUSTRY APPROACHES TO IP PROTECTION

Based on recent "off the record" interviews, companies take multiple approaches to protecting their IP. First, companies tightly control their research departments, with some limiting research to their headquarters where communication and controls can be monitored. Some U.S. companies that manufacture products offshore insist on having U.S. oversight in foreign plants at all times. Other companies only produce a "dumb box" outside the U.S., and don't add proprietary components until the product is in a tightly controlled domestic facility.

U.S. companies have also banded together via trade associations to help minimize IP piracy. The Software and Information Industry Association (SIIA) works with the education industry to provide classroom materials to teach students the dangers and costs associated with IP piracy. Additionally, the SIIA promotes amongst its members best practices for piracy prevention. Furthermore, the SIIA offers the ability to confidentially report piracy and then investigates and seeks restitution on behalf of its members.[176]

Off the record interviews in Washington, D.C. and in Silicon Valley revealed several of different approaches to the problem of frivolous lawsuits from PAEs. One firm in Silicon Valley noted that "patent trolls" were the biggest threat to IP, and that they aggressively sought their own patents to counter this threat. One trade association explained that they also viewed PAEs as a serious threat to IP, and that they lobbied for legal changes regarding the payment of costs during the discovery phase of IP cases.

Companies that value IP must also minimize the threat from insiders. Employees should be educated regularly about criminal phishing and social engineering schemes. Education plans should include company policies on using off-site email and data sharing applications. Furthermore, companies should conduct exit interviews to remind departing employees of laws regarding the ownership and sharing of corporate data.[177]

APPENDIX G: POLICY CONSIDERATIONS FOR FEDERAL IT PROCUREMENT

Despite spending almost $600 billion on information technology (IT) over the past decade, the federal government's IT portfolio has not kept pace with private sector IT advancements.[178] According to the OMB "Many Government IT projects cost hundreds of millions of dollars more than they should, take years longer than necessary to deploy, and deliver technologies that are obsolete by the time they are completed."[179]

With the national debt posing a threat to national security, it is imperative that the federal government get the best value from its IT systems.[180] To ensure this happens, the Obama administration has established policies to reduce IT costs, increase the rate of technology adoption, improve internal and external user experiences, enhance information security and privacy, and increase IT investment oversight and accountability. Additionally, the House of Representatives is working on legislation to reform federal IT acquisition.

IT policies issued by the legislative and executive branch can affect the ICT industry and government. For the ICT industry, IT policies produced since 2009 may result in unequal competitive advantage, reduced profitability, and higher barriers of entry. For the government, these same policies could produce service monopolies, security risks, and unfunded requirements. In both cases, these policy implications may counteract the benefits the administration and congress aim to achieve. To mitigate and minimize the impact of the previously outlined implications, Federal IT governance should:

- ***Align Agency IT Roadmaps with Commercial IT***: U.S. government buying power in the ICT industry has decreased as private sector and consumer ICT use has increased. As such, the U.S. government has little control over development of products and services in the industry. With the U.S. government lacking ICT buyer power, policy should drive agencies to align IT roadmaps with commercial IT roadmaps. Agencies should also be flexible enough to allow for adoption of unproven technologies.
- ***Mandate Outcomes for Federal IT, not Solutions***: Many of the IT policies issued by the current administration push for the adoption of specific IT solutions to achieve benefits. A better approach would be to establish performance goals for desired improvements. Policies should shift emphasis away from specified solutions to performance goals. This focus would give agency CIO's more flexibility and control over IT architectures and budgets, lower potential for monopoly services, decrease small business barriers, and keep CIO's from investing in solutions to simply fulfill statutory quotas.
- ***Maintain Competition in Federal IT***: In the ICT industry, when IT solutions with similar functionality exist, they are viewed as competing technologies not duplicative technologies. Competition can lead to lower prices and innovation. U.S. government policies should promote competition in federal IT and move away from the administration's current focus on eliminating duplicative IT solutions to simply minimizing duplication. To do this the federal government should set IT competition thresholds that must be met before agencies must "share first." Keeping duplicative services in the federal IT portfolio will help the government reap the benefits that come from healthy competition.

APPENDIX H: GLOSSARY

Advanced persistent threat (APT)	A type of cybercrime in which extraordinary amounts of our most sensitive data are stealthily siphoned in cyberspace and transferred abroad.[181]
Big data	This trend capitalizes on the vast amount of data—both structured and unstructured (i.e. videos, images, music and documents)—the world is generating, transmitting, and collecting digitally. It uses powerful algorithms, software applications, and computing capability—often enabled by in-memory processing—to "find the hidden pattern, the unexpected correlation, [or] the surprising connection" in mass amounts of data.[182]
Cloud computing	Cloud computing refers to the paradigm whereby data is stored, processed, and accessed across a network of Internet-accessible computers. This technology enables mass data storage and processing to be accomplished in ways never before envisioned. By shifting workload from local computers to a network of computers, which create a virtual "cloud," this new form of computing gives users access to data and applications on the Internet.[183] Virtualization of data centers, whereby software defined servers replace physical servers, is allowing greater computing capacities and efficiencies.
Industry value added (IVA)	"The value added of an industry, also referred to as GDP-by-industry, is the contribution of a private industry or government sector to overall GDP. The components of value added consist of compensation of employees, taxes on production and imports less subsidies, and gross operating surplus. Value added equals the difference between an industry's gross output (consisting of sales or receipts and other operating income, commodity taxes, and inventory change) and the cost of its intermediate inputs (including energy, raw materials, semi-finished goods, and services that are purchased from all sources)."[184]
Integrated circuit (IC)	An integrated circuit is a chip "composed of many interconnected transistors" A transistor is "a piece of silicon that amplifies electrical signals or serves as an on/off switch in computer applications."[185]
Internet protocol	"The Internet protocols are the world's most popular open-system (nonproprietary) protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications. The Internet protocols consist of a suite of communication protocols, of which the two best known are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The Internet protocol suite not only includes lower-layer protocols (such as TCP and IP), but it also specifies common applications such as electronic mail, terminal emulation, and file transfer."[186]
Mobility	While mobility is not a new trend, the "shift in consumer demand toward wireless products that offer the same functionality as wired

	products without the constraint of a fixed location" is continuing to transform the ICT industry.[187] Smartphones and, more recently, tablets have expanded the capability of mobile device computing while 4G network speeds are encouraging many users to completely abandon landlines.[188]
Patent assertion entities (PAEs)	Companies that purchase patents from non-practicing entities, such as universities, with no intent to use the patent in manufacturing and create revenue by suing innovators and manufacturers for patent infringement. While PAEs, known pejoratively as "patent trolls," provide much needed revenue to research centers, such as universities, many of their lawsuits are frivolous and cost the ICT industry billions of dollars annually.
Social networking platforms:	Social networking platforms are web-based services that allow people to digitally connect with others.[189] Externally these methods can be used for business marketing, delivery, and intelligence. Internally they can be harnessed for sharing information, building relationships, and collaboration.
Ubiquitous computing:	Leveraging capabilities provided by mobility and cloud, ubiquitous computing allows technology to "recede into the background of our lives" as everything that can benefit from connectivity is directly enabled with Internet protocol capabilities.[190] As such, ubiquitous computing is often referred to as the "internet of everything" or "everyware."[191] One of the most prominent examples of ubiquitous computing is the Google Glass system.[192]
Voice over Internet protocol (VoIP)	"A method for taking analog audio signals, like the kind you hear when you talk on the phone, and turning them into digital data that can be transmitted over the Internet."[193]
Wireless spectrum	"The wireless spectrum consists of electromagnetic radiation and frequency bands. Respective countries have their own wireless spectra with ranges up to 300 GHz. The wireless spectrum frequencies used in communication are regulated by national organizations, which specify which frequency ranges can be used by whom and for which purpose."[194]

[1] Schmidt, Eric and Jared Cohen. *The New Digital Age: Reshaping the Future of People, Nations and Business*. Kindle Edition. New York, NY: Alfred A. Knopf, 2013.

[2] Enriquez, Juan. "Reflections in a Digital Mirror." *The Human Face of Big Data*. Sausalito, CA: Against All Odds Productions, 2012, 19.

[3] Powell, Walter W. and Kaisa Snellman. "The Knowledge Economy." *Annual Review of Sociology*, 30 (August 2004), 199-220.

[4] The White House. "Cybersecurity." Accessed April 13, 2013, http://www.whitehouse.gov/cybersecurity.

[5] Totals calculated using data from the following reports:

a) Boyland, Kevin. *IBISWorld Industry Report 51913a: Search Engines in the US*. IBISWorld. Los Angeles, March 2013.

b) Boyland, Kevin. *IBISWorld Industry Report 51913b: Internet Publishing and Broadcasting in the US*. IBISWorld. Los Angeles, March 2013.

c) Schmidt, Dale. *IBISWorld Industry Report 51121: Software Publishing in the US*. IBISWorld. Los Angeles, March 2013.

d) Krabeepetcharat, Andrew. *IBISWorld Industry Report 54151: IT Consulting in the US*. IBISWorld. Los Angeles, April 2013.

e) Krabeepetcharat, Andrew. *IBISWorld Industry Report 51821: Data Processing & Hosting Services in the US*. IBISWorld. Los Angeles, February 2013.

f) Newsom, Caitlin. *IBISWorld Industry Report 33422: Communication Equipment Manufacturing in the US*. IBISWorld. Los Angeles, February 2013.

g) Krabeepetcharat, Andrew. *IBISWorld Industry Report 33411b: Computer Peripheral Manufacturing in the US*. IBISWorld. Los Angeles, March 2013.

h) Krabeepetcharat, Andrew. *IBISWorld Industry Report 33411a: Computer Manufacturing in the US*. IBISWorld. Los Angeles, January 2013.

i) Boyland, Kevin. *IBISWorld Industry Report 51711e: VoIP in the US*. IBISWorld. Los Angeles, December 2012.

j) Boyland, Kevin. *IBISWorld Industry Report 51332: Wireless Telecommunications Carriers in the US*. IBISWorld. Los Angeles, April 2013.

k) Boyland, Kevin. *IBISWorld Industry Report 51711d: Internet Service Providers in the US*. IBISWorld. Los Angeles, December 2012.

l) Boyland, Kevin. *IBISWorld Industry Report 51791a: Telecommunications Resellers in the US*. IBISWorld. Los Angeles, February 2013.

m) Boyland, Kevin. *IBISWorld Industry Report 51711c: Wired Telecommunications Carriers in the US*. IBISWorld. Los Angeles, March 2013.

n) Boyland, Kevin. *IBISWorld Industry Report 51741: Satellite Telecommunications Providers in the US*. IBISWorld. Los Angeles, October 2012.

o) Boyland, Kevin. *IBISWorld Industry Report 33421: Telecommunication Networking Equipment Manufacturing in the US*. IBISWorld. Los Angeles, February 2013.

[6] Totals calculated using data from IBISWorld reports: Ibid (a-d).

[7] Ibid.

[8] Ibid. 5 (e).

[9] Ibid.

[10] Totals calculated using data from IBISWorld reports: Ibid, 4 (f-h).

[11] Ibid.

[12] Ibid. 5 (h).

[13] Ibid.

[14] Ibid.

[15] International Data Corporation (IDC). "Worldwide HPC Market Update and Trends." In 23rd Daresbury Machine Evaluation Workshop: International Data Corporation (IDC), 2012.

[16] Totals calculated using data from IBISWorld reports: Ibid, 4 (i-o).

[17] Ibid.

[18] Ibid. 5 (i-k).

[19] Ibid. 5 (o).

[20] Ibid.

[21] Ibid.

[22] Strickland, Jonathan. "How Cloud Computing Works." *How Stuff Works*, accessed May 10, 2013. http://www.howstuffworks.com/cloud-computing/cloud-computing.htm.

[23] Ibid. 5 (h).

[24] Ibid. 5 (m).

[25] Ibid. 5 (n).

[26] Weiser, Mark. “Ubiquitous Computing.” Last modified March 17, 1996, accessed May 10, 2013, http://www.ubiq.com/hypertext/weiser/UbiHome.html.

[27] Kannav, Vikas. "Internet of Things." *Research @ Infosys Labs* (blog), July 31, 2012. http://www.infosysblogs.com/infosys-labs/2012/07/Internet of Things.html (accessed May 10, 2013).

[28] IBM. “What is a Smarter Planet?” Accessed April 18, 2013, http://www.ibm.com/smarterplanet/us/en/overview/ideas/index.html?re=sph.

[29] Boyd, Danah and Nicole B. Ellison. "Social network sites: Definition, history, and scholarship." *Journal of Computer-Mediated Communication*, 2007: 13(1), article 11, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

[30] Gardner, Dan. "An Ocean of Data." *The Human Face of Big Data*. Sausalito, CA: Against All Odds Publications, 2012, 15.

[31] TechAmerica Big Data Commission. "Demystifying Big Data: A Practical Guide to Transforming the Business of Government." TechAmerica Foundation. October 3, 2013. http://www.techamericafoundation.org/bigdata (accessed April 17, 2013).

[32] White, Martin. "Big Data-Big Challenges." *EContent* 34, no. 9 (2011): 21-21. http://search.proquest.com.ezproxy6.ndu.edu/docview/902758569?accountid=12686.

[33] Ibid.

[34] Presley, Theo. "Big Data Begs Us to Ask Bigger Questions of it." *WIRED*, April, 15, 2013, http://www.wired.com.ezproxy6.ndu.edu/insights/2013/04/big-data-begs-us-to-ask-bigger-questions-of-it/ (accessed April 15, 2013).

[35] Kalil, Tom. "Big Data is a Big Deal" *Office of Science and Technology Policy* (blog), March 29, 2012, accessed May 16, 2013, http://www.whitehouse.gov/blog/2012/03/29/big-data-big-deal.

[36] Seffers, George I. "U.S. Government Bets Big on Data." Signal 67, no. 5 (2013): 19-24. http://search.proquest.com.ezproxy6.ndu.edu/docview/1326239435?accountid=12686.

[37] TechAmerica Big Data Commission. "Demystifying Big Data: A Practical Guide to Transforming the Business of Government." TechAmerica Foundation. October 3, 2013. http://www.techamericafoundation.org/bigdata (accessed April 17, 2013).

[38] Ibid.

[39] Ibid.

[40] Ibid. 5 (h).

[41] Ibid. 5 (o).

[42] Reed, Brad. "Feds Move to Block AT&T-T-Mobile Merger." *Network World* (Online), Aug 31, 2011, http://search.proquest.com.ezproxy6.ndu.edu/docview/887523210?accountid=12686.

[43] Ibid. 5 (a, c)

[44] Ibid.

[45] Ibid. 5 (k-o).

[46] Ibid. 5 (h).

[47] Ibid.

[48] "The mobile app market uses "freemium," advertising, transaction and traditional paid business models…"
The "freemium" business model is one in which an app is offered for free with the option to pay for an upgrade to a premium version of the app that has improved functionality. The advertising model is earns revenue by selling

advertisements that are pushed to users via the app. The transaction model generates revenue when a user completes a transaction or makes a purchase. The paid business model generates revenue by selling the app itself to users. Maltz, Jules. "Choose Your Mobile Business Model Wisely". *WSJ Blogs* (blog). February 13, 2013, http://blogs.wsj.com/accelerators/2013/02/28/choose-your-mobile-business-model-wisely/ (accessed May 10, 2013).

"…while many large, established software publishing companies, including Microsoft and Adobe, are moving to subscription based sales models."
Ibid. 5 (c).

[49] Ibid. 5 (k).

[50] Ibid. 5 (l).

[51] Ibid. 5 (k).

[52] Council on Competitiveness. "U.S. Manufacturing—Global Leadership through Modeling and Simulation." Washington DC: Council on Competitiveness, 2009.

[53] Confidential Convergence Data Services, *Maximizing Your Company's Return on Data (RoD).* April 24, 2012, http://www.dscc.dla.mil/downloads/psmc/Apr12/12MaximizingReturnOnData.pdf (accessed April 5, 2013).

[54] Wyckoff, Andrew. *Knowledge is Growth*, Organization for Economic Cooperation and Development, 2013, http://www.oecd.org/innovation/knowledge-is-growth.htm (accessed 18 April 2013).

[55] Buchanan, Mark. *Nexus*: *Small Worlds and Groundbreaking Science of Networks*. New Yrok, NY: W.W. Norton and Company, 2002, 13.

[56] Smolan, Rick and Jennifer Erwitt, *The Human Face of Big Data*. First Edition, Sausalito, CA: Against all Odds Productions, 2012, 63.

[57] Ibid., p.11.

[58] The National Intelligence Council. *Global Trends 2025: A Transformed World*. November 2008, 68.

[59] Ibid.

[60] Federal Communications Commission. "What We Do." Accessed May 10, 2013, http://www.fcc.gov/what-we-do.

[61] As James Madison described in Federalist Paper 43, the U.S. public benefits when Intellectual Property (IP) is protected. In fact, the founding fathers viewed IP as so important to the wellbeing of the infant country, that they included IP protection in Article 1 of the constitution.
Clinton Rossiter, *The Federalist Papers*. New York, NY: Penguin Group, 2003, 268.

[62] U.S. Department of Commerce. *Intellectual Property and the U.S. Economy: Industries in Focus*, March 2012, http://www.uspto.gov/news/publications/IP_Report_March_2012.pdf.

[63] "Big Data." 2013.*Kirkus Reviews* LXXXI (5): n/a. http://search.proquest.com.ezproxy6.ndu.edu/docview/1312401227?accountid=12686.

[64] Office of E-Government & Information Technology, Office of Management and Budget *25 Point Implementation Plan to Reform Federal IT Management*, December 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/25-pointimplementation plan-to-reform-federal-it.pdf.

[65] Department of Homeland Security. "Critical Infrastructure Sector Partnerships." Accessed March 26, 2013, http://www.dhs.gov/critical---infrastructure---sector---partnerships.

[66] Umbach, Frank. "The U.S. ups investment in cybersecurity to halt hackers." *World Review*, Online Edition, April 11, 2013,http://www.worldreview.info/content/us-ups-investment-cyber-security-halt-hackers?goback= percent2Egde_3824763_member_231901274 (accessed April 19, 2013).

[67] Ibid.

[68] Ibid.

[69] Symantec Corporation. *2012 Norton Cybercrime Report*. 2012, 7.

[70] U.S. Congress. *HR 3523 as reported by the House Rules Committee*. Accessed May 7, 2013. http://www.rules.house.gov/Media/file/PDF_112_2/LegislativeText/CPRT-112-HPRT-RU00-HR3523.pdf

[71] Ibid. 69.

[72] Ibid. 6.

[73] Mandiant. *APT1 – Exposing One of China's Cyber Espionage Units*. February 2013, 3.

[74] Damballa, "What's an APT? A Brief Definition," accessed May 8, 2013, https://www.damballa.com/knowledge/advanced-persistent-threats.php.

[75] Ibid. 73, p. 2.

[76] Ibid. 73, p. 3.

[77] Ibid.

[78] Ibid. 73, p. 40.

[79] Ibid. 73, p. 3.

[80] Ibid. 73, p. 4.

[81] Ibid. 73, p. 23.

[82] Ibid. 73, p. 3.

[83] Ibid. 73, p. 3.

[84] Ibid. 73, p. 52.

[85] Ibid. 73, p. 60.

[86] Department of Defense. *Annual Report to Congress - Military and Security Developments Involving the People's Republic of China 2013*. May 2013: 36.

[87] U.S. Department of Commerce. "Stolen Intellectual Property Harms American Businesses Says Acting Deputy Secretary Blank," *The Commerce Blog* (blog), Nov 29, 2011, http://www.commerce.gov/blog/2011/11/29/stolen-intellectual-property-harms-american-businesses-says-acting-deputy-secretary- (accessed May 13, 2011).

[88] "Triumph of the Nerds: The Rise of Accidental Empires," PBS (transcript), http://www.pbs.org/nerds/part3.html (accessed May 16, 2013).

[89] Verizon. *DBIR Snapshot: Intellectual Property Theft*. 2012, 2-3.

[90] Symantec. *What's Yours is Mine: How Employees are Putting Your Intellectual property at Risk*, Mountain View, CA: Symantec, 2013, 1, http://www.idgconnect.com/download/13315/what-yours-mine-how-employees-putting-your-intellectual-property-risk?contact_id=49fe1ce44a3bf1104191d7738755a540&source=USNL041213a (accessed May 16, 2013).

[91] U.S. Trade Representative. "USTR Releases Annual Special Section 301 Report on Intellectual Property Rights," Office of the USTR Website, April 2012, http://www.ustr".gov"/about-us/press-office/press-releases/2012/april/ustr-releases-annual-special-301-report-intellectual.

[92] Wilson, Chrisopther E. "Some Light Shed on 'Patent Trolls,'" *TechAmerica Policy Blog* (blog), Dec 11, 2012, http://www.techamerica.org/some-light-shed-on-patent-trolls/.

[93] Brown, Evelyn. "October Workshop to Consider Future of Information and Communication Technology Supply Chain Risk Management," *NIST Tech Beat*, September 18, 2012, http://www.nist.gov/itl/supply-091812.cfm (accessed May 8, 2013).

[94] Levin, Carl. *Opening Statement at SASC Hearing on Counterfeit Electronic Parts in DoD Supply Chain*, November 8, 2011, http://www.levin.senate.gov/newsroom/speeches/speech/opening-statement-at-sasc-hearing-on-counterfeit-electronic-parts-in-dod-supply-chain (accessed April 18, 2013).

[95] U.S. Senate. *Report of the Committee on Armed Services*: *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, May 21, 2012: iv, http://www.armedservices.senate".gov"/Publications/Counterfeit percent20Electronic percent 20Parts.pdf.

[96] *National Defense Authorization Act for Fiscal Year 2012*, *Conference Report to Accompany H.R. 1540*. December 12, 2011, Section 818, http://www.gpo".gov"/fdsys/pkg/CRPT-112hrpt329/pdf/CRPT-112hrpt329-pt1.pdf.
See also, Robert S. Metzger and Jeffery M. Chiow, "DoD's Counterfeit Parts Rule is Coming Soon." *RJO Update: Government Contracts*, June 2012 http://www.rjo.com/updatesDoDcounterfeitpartsrule.html (accessed April 18, 2013).

[97] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Defense Science Board Task Force on High Performance Microchip Supply*, February 2005: 14, http://www.acq.osd.mil/dsb/reports/ADA435563.pdf.

[98] Ibid.

[99] Goldman, David. "Fake tech gear has infiltrated the U.S. government." *CNNMoney*, Nov 8, 2012: 1, http://money.cnn.com/2012/11/08/technology/security/counterfeit-tech/index.html.

[100] Poitras, Colin. "Conference on Counterfeit Electronics Addresses Growing National Concern," *UConn Today*, February 1, 2013, http://today.uconn.edu/blog/2013/02/conference-on-counterfeit-electronics-addresses-growing-national-concern/ (accessed April 18, 2013).

[101] Mundy, Simon and Sarah Mishkin, "Falling prices to be just a memory for chip manufacturers," *Financial Times* (Online Edition) May 6, 2013, http://www.ft.com/cms/s/0/b10b96f2-b539-11e2-ace9-00144feabdc0.html#axzz2ShPwyDER (accessed May 8, 2013).

[102] Ibid.

[103] Milan, Mark. "How a Major Conflict in Korea Could Ripple Through Mobile Industry," *Bloomberg-Global Tech*, May 6, 2013, http://www.bloomberg.com/news/2013-05-06/a-major-conflict-in-korea-could-disrupt-phone-production.html (accessed April 18, 2013).

[104] Drew, Christopher. "Why Science Majors Changes Their Mind (Its Just so Darn Hard)", *The New York Times*, November 4, 2011, http://www.nytimes.com/2011/11/06/education/edlife/why-science-majors-change-their-mind-its-just-so-darn-hard.html?pagewanted=all&_r=0 (accessed April 18, 2013).

[105] Ibid.

[106] Ibid.

[107] Wright, Josh. "Information Technology: Lots of Jobs Available, But Enough IT Workers To Fill Them?" *EMSI Blog* (blog), March 11, 2013, http://www.economicmodeling.com/2013/03/11/information-technology-lots-of-jobs-available-but-enough-it-workers-to-fill-them/ (accessed on April 5, 2013).

[108] Wright, Josh. "An IT Worker Shortage? It Depends on the State" *EMSI Blog* (blog), September 26, 2012, http://www.economicmodeling.com/2012/09/26/an-it-worker-shortage-it-depends-on-the-state/ (accessed April 16, 2013).

[109] Ibid.

[110] Alden, Edward. "America's National Suicide." *Newsweek*, April 10, 2011, http://www.thedailybeast.com/newsweek/2011/04/10/america-s-national-suicide.html (accessed April 18, 2013).

[111] "The Jobs Machine." *The Economist*, April 13-19, 2013, 63.

[112] Aarti, Shahani. "Why Silicon Valley Is Losing Foreign-Born Talent", KQED, Public Media for Northern California, March 21, 2013, http://blogs.kqed.org/newsfix/2013/03/21/is-silicon-valley-losing-its-foreign-talent/ (accessed April 5, 2013).

[113] Savitz, Eric, "The Solution To The Wireless Spectrum Shortage," *CIO Network* (blog), March 23, 2012, http://www.forbes.com/sites/ciocentral/2012/03/23/the-solution-to-the-wireless-spectrum-shortage-more-wires/ (accessed May 16, 2016).

[114] Ibid.

[115] Ibid.

[116] Ibid.

[117] Subramanian, Rangam. "Avoiding the Spectrum Crunch: Growing the Wireless Economy Through Innovation," statement before The House Committee on Science, Space, and Technology, April 18, 2012.

[118] Goldstein, Gordon. "The fight to keep a state-free internet." *Financial Times* (online edition), December 16, 2012, http://www.financialtimes.com (accessed March 1, 2013).

[119] Blue, Violet. "UN plans Internet governance amid outcry to defend ITU." *Pulp Tech*. Jan 16, 2013, http://www.zdnet.com/un-plans-internet-governance-amid-outcray-do-defend-itu-70000098 (accessed Mar 10, 2013).

[120] Waters, Richard, Daniel Thomas, and James Fontanella-Khan. "Fears grow over efforts to govern the web." *Financial Times* (online edition), November 28, 2012, http://www.financialtimes.com (accessed March 10, 2013).

[121] Federal Communications Commission. "Open Internet." Accessed May 16, 2012, http://www.fcc.gov/openinternet.

[122] Ibid.

[123] According to the *National Security Strategy*, our national interests are: "The security of the United States, its citizens, and U.S. allies and partners; a strong, innovative, and growing U.S. economy in an open international economic system that promotes opportunity and prosperity; respect for universal values at home and around the world; and an international order advanced by U.S. leadership that promotes peace, security, and opportunity through stronger cooperation to meet global challenges."
The White House. *National Security Strategy.* May 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[124] Clinton, Hilary Rodham. "Conference on Internet Freedom Remarks." Last modified December 8, 2011, accessed May 12, 2013, http://www.state.gov/secretary/rm/2011/12/178511.htm.

[125] Gibson, William. "The Science in Science Fiction." *National Public Radio*, November 30, 1999.

[126] IBM, "Reference FAQ." Accessed April 4, 2013, http://www-03.ibm.com/ibm/history/reference/faq_0000000011.html.

[127] Friedman, Thomas. "How America Fell Behind." *National Public Radio*, September 6, 2011.

[128] Petroski, Henry. "Distinguishing Between Scientists & Engineers." *Design News*, March 10, 2011, http://www.designnews.com/document.asp?doc_id=233915&dfpPParams=aid_233915&dfpLayout=article&dfpPParams=aid_233915&dfpLayout=article (accessed May 5, 2013).

[129] Federal Bureau of Investigation. *Addressing Threats to the Nation's Cybersecurity*. Accessed April 6, 2013, http://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1.

[130] Jackson, William. "Napolitano: Cyber threat 'right in front of us.'" *GCN*, March 23, 2012. Accessed April 1, 2013, http://gcn.com/Articles/2012/03/23/DHS-2013-budget-cyber-threat-senate-hearing.aspx?Page=3

[131] Ibid.

[132] National Telecommunications & Information Administration. "Public Safety." Accessed April 1, 2013, http://www.ntia.doc".gov"/category/public-safety

[133] U.S. Department of Energy. "Mission." Accessed May 17, 2013, http://www. http://energy.gov/mission.

[134] IBM. *TerraEchos: Streaming data technology supports covert intelligence and surveillance sensor systems*. May 2012: 1, http://terraechos.pyratetech.com/PDFs/47245_TerraEchos%20Streaming%20data_Case%20Study_IMC14726-USEN-01_Final_Jun4_12.pdf (accessed May 17, 2013).

[135] Ibid.

[136] Ibid.

[137] Ibid., p. 5.

[138] Ibid., p. 2.

[139] Ibid.

[140] Ibid.

[141] Ibid., p. 4.

[142] Department of Homeland Security. *Privacy Impact Assessment EINSTEIN Program: Collecting, Analyzing, and Sharing Computer Security Information Across the Federal Civilian Government*. September 2004, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf.

[143] The White House. "The Comprehensive National Cybersecurity Initiative." Accessed April 6, 2013, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[144] Department of Defense, *Department of Defense Information Enterprise Architecture (DoD IEA) Version 2.0*. July 2012, http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD%20IEA%20v2.0_Volume%20I_Description%20Document_Final_20120730.pdf (accessed May 16, 2013).

[145] Department of Defense, "Build and Operate a Trusted GIG. Cyber, Identity and Information Assurance (CIIA) Related Policies and Issuances." Last modified April 25, 2013, accessed May 13, 2013. http://iac.dtic.mil/csiac/download/ia_policychart.pdf.

[146] Ibid. 144.

[147] Defense Information Systems Agency. *Strategic Plan: 2013-2018*. Version 1.0, http://www.disa.mil/About/~/media/Files/DISA/About/Strategic-Plan.pdf.

[148] Office of Management and Budget. *OMB Memorandum M-09-32: Update on the Trusted Internet Connections Initiative*. September 17, 2009, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/m09-32.pdf.

[149] Office of Management and Budget. *OMB Memorandum M-10-06: Open Government Directive*. December 8, 2009, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf.

[150] Office of Management and Budget. *OMB Memorandum M-10-22: Guidance for Online Use of Web Measurement and Customization Technologies.* June 25, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf.

[151] Office of Management and Budget. *OMB Memorandum M-10-26: Guidance for Agency Use of Third-Party Websites and Applications*. June 25, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

[152] Office of Management and Budget. *OMB Memorandum M-10-25: Reforming the Federal Government's Efforts to Manage Information Technology Projects*. June 28, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m_10-25.pdf.

[153] Office of Management and Budget. *OMB Memorandum M-10-26: Immediate Review of Financial Systems IT Projects.* June 28, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m-10-26.pdf.

[154] Office of Management and Budget. *OMB Memorandum M-10-27: Information Technology Investment Baseline Management Policy*. June 28, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-27.pdf.

[155] Office of Management and Budget. *OMB Memorandum M-10-31: Immediate Review of Information Technology Projects.* June 28, 2010, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2010/m10-31.pdf.

[156] Office of Management and Budget. *OMB Memorandum M-10-32: Evaluating Programs for Efficacy and Cost Efficiency*. July 29, 2010, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2010/m10-32.pdf.

[157] Office of Management and Budget. OMB Memorandum M-11-02: *Sharing Data While Protecting Privacy*. November 3, 2010, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-02.pdf.

[158] Office of E-Government & Information Technology, Office of Management and Budget. *25 Point Implementation Plan to Reform Federal IT Management*. December 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/25-point-implementation-plan-to-reform-federal-it.pdf.

[159] Office of Management and Budget. *OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors*. February 3, 2011, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.

[160] Office of E-Government & Information Technology, Office of Management and Budget. *Federal Cloud Computing Strategy*. February 8, 2011, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

[161] The White House. *Executive Order 13571: Streamlining Service Delivery and Improving Customer Service*. April 27, 2011, http://www.whitehouse".gov"/the-press-office/2011/04/27/executive-order-streamlining-service-delivery-and-improving-customer-ser.

[162] The White House. *Executive Order 13576: Delivering an Efficient, Effective, and Accountable Government*. June 13, 2011, http://www.whitehouse".gov"/the-press-office/2011/06/13/executive-order-delivering-efficient-effective-and-accountable-governmen.

[163] Office of Management and Budget. *OMB Memorandum M-11-27: Implementing the Telework Enhancement Act of 2010, Security Guidelines.* July 15, 2011, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-27.pdf.

[164] Office of Management and Budget. *OMB Memorandum M-11-29: Chief Information Officer Authorities*. August 88, 2011, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf.

[165] The White House. *Executive Order 13587: Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.* April 27, 2011, http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks-.

[166] The White House. *Executive Order 13589: Promoting Efficient Spending*. November 9, 2011, http://www.whitehouse.gov/the-press-office/2011/11/09/executive-order-promoting-efficient-spending.

[167] Office of Management and Budget. *OMB Memorandum M-12-10: Implementing PortfolioStat*. March 30, 2012, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-10.pdf.

[168] Office of E-Government & Information Technology, Office of Management and Budget. *Federal Information Technology Shared Services Strategy*. May 2, 2012, http://www.whitehouse".gov"/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf.

[169] Office of Management and Budget. *OMB Memorandum: Increasing Shared Approaches to Information Technology Services*. May 2, 2012, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/sharedapproachmemo_0502.pdf.

[170] Office of Management and Budget. *The Common Approach to Federal Enterprise Architecture*. May 2, 2012, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf.

[171] Office of E-Government & Information Technology, Office of Management and Budget. *Digital Government Strategy*. May 23, 2012, http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html.

[172] Office of Management and Budget. *OMB Memorandum M-13-02: Improving Acquisition through Strategic Sourcing*. December 5, 2012, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-02_0.pdf.

[173] Ibid.

[174] Office of Management and Budget. *OMB Memorandum M-13-08: Improving Financial Systems through Shared Services*. March 25, 2013, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-08.pdf.

[175] Office of Management and Budget. *OMB Memorandum M-13-09: Fiscal Year 2013 PortfolioStat Guidance: Strengthening IT Portfolio Management*. March 27, 2013, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf

[176] Software and Information Industry Association. "Intellectual Property." Accessed April 18, 2013, http://siia.net/index.php?option=com_content&view=article&id=642:intellectual-property&catid=163:public-policy-articles&Itemid=711.

[177] Ibid. 90.

[178] Office of E-Government & Information Technology, Office of Management and Budget. *25 Point Implementation Plan to Reform Federal IT Management*. December 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/25-pointimplementation plan-to-reform-federal-it.pdf.

[179] Office of Management and Budget. *OMB Memorandum M-10-25: Reforming the Federal Government's Efforts to Manage Information Technology Projects*. June 28, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m_10-25.pdf.

[180] Marshall, Tyrone C., Jr. "Debt is Biggest Threat to National Security, Chairman Says." *American Armed Forces Press Service*, September 22, 2011, http://www.defense.gov/news/newsarticle.aspx?id=65432 (accessed May 16, 2013).

[181] Ibid. 73.

[182] Ibid. 30.

[183] Ibid. 22.

[184] Bureau of Economic Analysis, U.S. Department of Commerce. "What is industry value added?" accessed May 16, 2013, http://www.bea.gov/faq/index.cfm?faq_id=184.

[185] Soclof, Sidney. "How Circuits Work." *How Stuff Works*, accessed May 16, 2013, http://www.howstuffworks.com/environmental/energy/circuit5.htm.

[186] Cisco. "Internet Protocols." Accessed May 16, 2013, http://docwiki.cisco.com/wiki/Internet_Protocols.

[187] Ibid. 5 (m).

[188] Ibid. 5 (j).

[189] Ibid. 29.

[190] Ibid. 26.

[191] Ibid. 27.

[192] Ibid. 28.

[193] Valdes, Robert and Dave Roos. "How VoIP Works." *How Stuff Works*, accessed May 16, 2013, http://www.howstuffworks.com/cloud-computing/cloud-computing.htm.http://www.howstuffworks.com/ip-telephony.htm.

[194] Jansse, Cory. "Wireless Spectrum." *Techopedia*, accessed May 16, 2013, http://www.techopedia.com/definition/27409/wireless-spectrum.