# Principles for Creating an Economically Stable and Cyber-Secure European Union


**Internet Security Alliance For Europe (ISAFE)**

INTERNET SECURITY ALLIANCE FOR EUROPE

## EXECUTIVE SUMMARY

The future vitality of the European economy is dependent on maintaining a vibrant and functional Internet structure. This means that debate over the appropriate steps to secure the Internet must be considered not through a narrow set of requirements, but in context of broader economic issues.

Our information systems are under attack with methods at times so sophisticated that major corporations and even powerful governments are unable to prevent penetration. Our goal must be not just to enhance the security of our networks but also to do so in a fashion that will allow for, and encourage, the innovation, growth and competitiveness of EU based companies and national economies.

To achieve these goals he Internet Security Alliance For Europe (ISAFE), a pan-European coalition of major enterprises from multiple sectors, propose structuring the EU directive for cyber security based on the 5 basic principles:

1. The enormous and growing cyber threat to industry must be understood primarily as an economic attack wherein the attacking community has massive advantages over the victims of these, sometimes nation-state supported, attacks.
2. Traditional EU regulatory approaches and timescales are[ISA1] ill-suited as a method to address the realities of 21st century cyber attacks
3. Over regulation in this space not only won't enhance security but will have substantial negative economic impacts on EU industry and member states at a time when we can least afford it
4. We should establish a "cyber security social contract" between EU industry and government to promote collaborative security and economic growth
5. Following a primarily regulatory model in the EU will place EU based companies at a competitive disadvantage thus hurting EU economic growth

INTERNET SECURITY ALLIANCE FOR EUROPE

1. **The enormous and growing cyber threat to industry must be understood primarily as an economic attack wherein the attacking community has massive advantages over the victims of these, sometimes nation-state supported, attacks.**

The cyber threat is real, serious and growing and multi-dimensional. According to the Canter for Strategic and International Studies, cyber crime costs hundreds of billions of dollars a year and both the number of attacks and the impact they are having is growing rapidly and will continue to do so. [i] Various government entities have warned of the capability to attack and disable critical national infrastructure through cyber means. [ii] Furthermore, while many cyber attacks are relatively unsophisticated the percentage of attacks employing multiple means and increased sophistication is growing rapidly and even comparatively basic attacks, when confronted by basic effective defensive measures are escalated to increasingly sophisticated methods until the attacker's goal is achieved. [iii]

Cyber attacks can be classified in many ways however one useful distinction might be to separate the "military" attacks from the criminal attacks. For the purposes of this paper we will define the "military" style of cyber attack as those with traditional military style goals such as the destruction or disruption of critical infrastructure.

A second discrete category of attacks is best thought of as "criminal" wherein the purpose is not to destroy persons or property but rather to generate some sort of economic gain for the attacker. Examples of this would be theft of intellectual property or business processes.

Both types of attack are serious and in need of attention. However the nature of an attack designed to destroy critical infrastructure may be quite different from one designed to use the critical infrastructure for ongoing thievery. This paper will focus on addressing the attacks that are economic in nature.

According to at least some published Intelligence estimates the types of attacks designed to cripple critical infrastructure are, at least for the time being of comparatively little likelihood of occurring[ISA2].

This is because up to 95% of current cyber attacks are economic in nature. [iv] These economic attacks are having a devastating effect on private industry as well as the nations within which the private enterprises reside. For example it is estimated that the G 20 economies have already lost 2.5 million jobs due to counterfeiting and piracy and that governments and consumers experience US $125 billion in losses including tax revenue each year. TNO, the Dutch

research organization, has reported that cyber crime cost Dutch society at least 10 billion Euros per annum, which is 1.5 to 2% of their national GDP. Other studies in Germany and the UK indicate similar losses. [vvi]

An oft heard, and fundamentally flawed, observation is that these attacks on private industry reflect poor judgement or selfishness on the part of industry that care about profits and not security. However, no business is interested in losing such massive amounts of money on a perennial basis, and in fact studies indicate that in the last half decade corporate spending on cyber security has increased as much as 500%, and yet the problem still grows. [vii]

Blaming the corporate victims of these attacks and threatening them sever penalties reflects a fundamental misunderstanding of the cyber security issue. Defending against modern cyber attacks is so difficult even nation-states cannot guarantee the security of their systems. Moreover cyber defence difficult and getting harder for several reasons.

First, the attackers are getting much more sophisticated. The sort of ultra-sophisticated attacks (the so called Advanced Persistent Threat or APT) style methods that we saw confined to nation state on nation state attacks just a few years ago are not being practiced throughout the economy by common criminals [viii] ---sometimes the attacks are supported by nation states intent on stealing corporate IP and business process to assist their own domestic industries.[ixx] It is unreasonable to expect private corporations to defend themselves adequately from attacks by, or supported by, nation states.

Second, our information systems are becoming ever more vulnerable. The Internet was initially designed without security in mind and now with the explosion of mobile devices, the popularity of BYOD, and the coming Internet of Things the systems are becoming ever more open and vulnerable

Third, the economics of cyber security all favor the attackers. Even sophisticated attacks are comparatively cheap, easy to access and the profit margins for the criminals are enormous. On the defense side our strategies is almost inherently a generation behind that of the attackers we have to respond to. In addition, international competition is driving industry to adopt new business practices such as the use of long international supply chains or technologies such as cloud computing which raise new difficult and costly challenges to security. And finally, there is virtually no effective law enforcement ---we successfully prosecute maybe 1 or 2 % of cyber criminals.[xi]

In short, EU industry, already faced with one of the most difficult economic environments in the last 70 years, must now grapple with an extraordinarily complex set of technical, political and economic issues as it attempts to secure the information systems upon which their own competitiveness as well as that of their home nation's, rests. EU industry needs a partnership with its government not threats and punishment while fighting attackers that even the governments themselves have not shown they can combat effectively.

2. **Traditional EU regulatory approaches and timescales are**[ISA3] **ill suited as a method to address the realities of 21st century cyber attacks.**

Obviously there will be some elements of regulation associated with EU action on cyber space. For example, citizens who have their personal data compromised need to be informed of these attacks and this system will be most effective if uniformly applied across EU nation states. In addition, industries where the fundamental economics of the industry are inherently directed from a regulatory structure can use that structure to motivate additional security practices.

Moreover, there already exists substantial regulation within key sectors relating to cyber security. The most critical steps policy makers can take with respect to this existing regulation, both from an economic competitiveness as well as a security perspective, is to assure that entities providing similar services are regulated equally. As digitalization and other factors create new competitive platforms, policy makers can streamline and reduce regulatory burdens for those entities who demonstrate enhanced security practices.

However, outside of these unique circumstances the traditional model alone cannot be relied on to provide an effective or sustainable system of cyber security. The digital world in general is different, and the cyber security landscape is particularly different. Digital technology tends not to fit well into traditional regulated categories, which makes compliance and enforcement difficult. The technology changes almost constantly and is deployed very differently by users with major differences apparent even within single corporate structures.

Unfortunately, the current EU draft NIS Directive relies on this outdated regulatory approach, originally designed to meet the challenges of the 18th century. These models are too slow and cumbersome to manage the digital environment of the 21st century. They will probably not be effective, and they could even undermine our ability to create a sustainable system of cyber defence.

In the traditional regulatory model, a government agency determines requirements, which are then mandated upon citizens and businesses. Among the reasons this model does not fit well as a method to address cyber threats are:

- Attack methods vary widely and change almost constantly, so that it is difficult to keep the regulations responsive to current threats.
- Compliance with outdated or ineffective regulations can be costly and time-consuming without adding significantly to actual security.[xii] In fact, it may divert scarce security resources away from emerging threats. One immutable truism of digital defence is that we simply do not have enough capable cyber security practitioners. Corporations are faced with fighting off multiple persistent and ever evolving threats with limited and highly stressed personnel. When that limited personnel is pulled of actual security to address complex, and almost assuredly out of date, government requirements they have less time and attention to spend on actual security.
- The attribution of cyber-attacks is extremely difficult and assigning liability is unreliable. Cyber systems as well as attack methods traverse traditional national boundaries and it can be difficult to establish jurisdiction. Indeed, an overly broad assertion of jurisdiction can drive commerce toward more accommodating domains and cause economic disruption.
- Traditional regulatory procedures, such as disclosure can also be counterproductive to security. While disclosure of personal data breaches is required, disclosure of security events with the intent to draw the attention of the public[ISA4] , potentially affecting an organization's stock price, can be counterproductive. We are already aware of instances wherein attackers have used cyber attacks to manipulate stocks and generate ill-gotten revenues.
- Information sharing programs should voluntary and carefully tailored to meet security needs. Modern cyber attacks are often stealthy. It typically takes over a month to discover many attacks and the methods to uncover such attacks are often costly and as much art as science. Corporations need to WANT to discover these attacks and government needs to be sharing on an equivalent basis.

3. **Cyber regulation will not enhance security but will have substantial negative economic impact on EU industry.**

The European Union has suffered from major economic decline in recent years, and this trend may well continue. The World Bank expects inflation to continue to rise, but fears that in these uncertain times there is also the potential for a major deflation event, which could cripple to stability of the European Central Bank. [xiii]

One study estimates that infrastructure modernization, which relies on information systems, will account for up to 46% of the global economy over the next 10 years[xiv] making cyber policy a central feature for economic growth. Against this uncertain economic backdrop and with the massive potential for stimulating EU economic growth with productive cyber policies the current heavily regulatory direction of the EU cyber directive seems out of step with broader EU needs.

There is a diverse and well-developed research precedent identifying effect that regulatory policies may have on stifling innovation, investment and productivity.

One recent work, *The Economic Effects of the Regulatory Burden*, found that the long-term burden of regulation on businesses creates a profound negative economic impact. Regulations to businesses ultimately make development and production difficult in the long run, with costs reaching beyond direct, administrative costs. Tight regulations make it problematic for businesses to adapt to environmental changes. To a lesser extent, regulatory burden of businesses also has a negative impact on entrepreneurship and investment. Fewer entities have the ability to enter the market, which decreases competition and stifles creative solutions. [xv]

Similar findings were reported in *Greasing the Wheels? The Impact of Regulations and Corruption on Firm Entry*. Data from the World Bank was used to conduct research on France, Germany, and the UK. The study concludes that "regulations robustly deter firm entry into markets. Greater procedural burdens and increased capital requirements dissuade entrepreneurs from engaging in business development activities and encumber new businesses from market entry. [xvi]

Focusing more directly on the regulatory impact in Internet industries another recent study found that that more stringent digital content copyright regulations in the European Union would negatively impact early-investments in digital content intermediaries …Our European study results generally fall in line with those from the United States. More stringent regulations of intermediaries would deter many [venture capitalists] from investing in the space." [xvii]

While there is not at this time a set of cyber security specific studies on the economic effects of regulation there is little to suggest that the regulatory effects of the current EU draft Directive is likely to have the same negative economic impacts that other regulations in similar spaces have experienced.

Especially considering, as we have already detailed, that regulation in this space is unlikely to enhance security due to the unique characteristics of the Internet and digitalization, consideration of an alternative approach to the traditional regulatory models is appropriate. To actually increase security, this alternative approach needs to be outcome-focused and must appreciate the impact on industry. If the commission were to come up with a robust plan for how reported information will be exploited, and how it will be used to better inform market operators' approaches to cyber security, and then uses this view to inform the implementation of the directive (thresholds for reporting etc) this could add value[ISA5].

4. **We should establish a "cyber security social contract" between industry and government to promote collaborative security and economic growth**

Modern cyber attacks demand a more flexible and dynamic model to address the enormous and unfamiliar challenges that arise from the ubiquitous nature of digital technology and the inherent vulnerabilities that come with it. These challenges are simply too complex for governments or individual companies to manage alone. Even if organizations do an excellent job they can be compromised by deficiencies in any of the multitude of systems with who they are interconnected. We can no longer seek only to secure our own networks. We need to work collaboratively to create a more secure system.

In 2008 ISAFE's US affiliate, the Internet Security Alliance, published an alternative model "The Cyber Security Social Contract" [xviii] which called for a new partnership between governments and the industry. The Cyber Social Contract proposed that industry and government work collaboratively to identify effective standards and practices for cyber security. Once these elements of sound cyber management were mutually identified the model called for individual entities to choose the practices and standards that would best fit their unique cyber risk profile. Since it was understood that governments may desire levels of security that exceeded the commercial needs of individual corporations and that research has consistently shown that the number one barrier to enhanced cyber security is cost, [xix] the model suggested governments could motivate higher levels of cyber security by deploying a set of market incentives.

In the US the Obama Administration initially proposed a traditional, government centric, regulatory model --- not dissimilar from the current EU Directive ---wherein government would set cyber security mandates for industry with the prospect of heavy penalties for non-compliance. Despite the fact that President Obama's party controlled the US Senate, he could not generate sufficient support even within his own party (largely due to the issues raised under principles 2 & 3 above) to even bring his proposal to a vote in a Senate Committee, which is usually a pro forma step for the party in power in the US Senate.

Subsequently the Obama Administration has abandoned their regulatory proposals and instead adopted the principles embodied in the Cyber Security Social Contract. In fact the Social Contract publication was the first and most often referenced source in the President's primary policy paper on cyber Security "The Cyber Space Policy Review." [xx]

More importantly, in 2013 President Obama issued an Executive Order 13636[xxi] for the US federal government to implement the core tenants of the Social Contract model. The National Institute for Standards and Technology (NIST) was designated to work with the private sector to develop the Framework of standards and practices. [xxii] Following the development of the NIST Framework the Administration has launched a multi-faceted effort to develop appropriate market incentives to promote voluntary use of the principles outlined in the Framework. [xxiii]

The Administration has repeatedly, and explicitly, asserted that it will not seek any new regulatory authority for cyber security [xxiv]. In addition several of the US regulatory bodies including the Federal Communications Commission [xxv] [xxvi]and the Department of Energy[xxvii] have publically expressed their views as to how well the collaborative efforts are going and their preference for this approach over traditional regulation.

ISAFE proposes the EU consider a similar, social contract approach for the EU. EU industry and government and industry would develop new and expanded roles in working together against cyber threats. Industry, which has greater cyber security expertise than most governments would be primarily responsible for working to develop standards and practices and government, would be responsible for motivating voluntary adoption of increased security practices through deployment of market incentives

It must be noted that the incentive programs anticipated will of pragmatic necessity need not to create significant financial costs for already strapped governments. However there are a wide range of incentive programs that cost governments little if anything but may generate attractive economics for the private sector who voluntarily elevate security. Among these

incentive programs are streamlined or preferential regulatory policies, patent processes, insurance, government procurement, technical assistance and intensified government collaboration for voluntary good actors who meet of exceed mutually identified preferred levels of security.

5. **Following a primarily regulatory model in the EU will place EU based companies at a competitive disadvantage & hurt EU economic growth**

We now work in a world economy. Even if EU based companies' focus primarily on the EU market, operating under more extensive regulations than their competitors is likely to undercut their productivity, job creation and innovation. This is especially concerning if, as in the current case, there is no evidence that the regulatory provisions of the EU directive will materially improve security.

Corporations located in Asia and North America will almost certainly operate under less costly and burdensome environments than EU based entities if the current Directive is enacted. Even if these companies have to adapt to EU requirements when providing services within the EU, they will have more competitive base environments from their home locations making them more competitive. Some non-EU based entities may actually choose not to provide service within the EU if the overhang of EY regulatory structures and penalties is judged not a prudent investment. Such a possibility threatens to deprive EU citizens and companies access to the full world market and will result in EU citizens being captive to fewer market choices and in all likelihood higher prices for services.

Not only will these enterprises have less regulatory overhang than EU based companies but there is ample evidence that at least some eastern European and Asian nations are actually using cyber incursions to benefit their own domestic businesses. The US, while not as aggressive, are planning to deploy market incentives for cyber security rather than inflicting costly new regulations and penalties for non-compliance. If the EU cyber directive proceeds as currently planned with its extensive new regulations and penalties EU companies will increasingly be placed at a competitive disadvantage *vis-à-vis* their US and Asian counterparts.

The US Congress has adjourned for the year without passing any cyber security legislation. This virtually assures that the voluntary incentive model, will remain US policy for at least the next few years and likely beyond. Even the regulatory review the Administration is undertaking is designed to streamline and condense regulations not add new ones. [xxviii]With few possible exceptions in discrete economic sectors the US system is liable to be fairly stable.

As a result US based companies can look forward to and plan investment decisions, confident that new cyber regulatory burdens and requirements will not be added. Moreover, with increased economic motives to practice good security American companies are liable to become increasingly secure in comparison to their EU counterparts making them more attractive business partners and magnets for outside investment.

Among the unique burdens EU companies will have to face under the current directive are:

1. Stakeholders are to report to a 'national competent authority' (NCA) responsible for enforcing the Directive. Such a requirement will likely create a minimalist approach with companies focused only on what is the minimum needed to be in compliance rather than what is needed to manage cyber threats based on their own risk profile. There is no similar requirement for US, Russian and most Asian companies. Rather, US firms are being incentivized to expand their cyber risk management in response to their unique cyber risk profiles. And other national states are providing more aggressive assistance to their domestic firms. In addition the reporting procedures in the EU will likely often be a duplicative burden resulting in redundant reporting that will take away scarce security resources and divert them to redundant compliance.
2. Member States will impose requirements that 'guarantee a level of security appropriate to the risk presented'. In reality no entity can guarantee cyber security and member states do not have the knowledge or resources to accurately assess what the appropriate risk is for a private enterprise. It is very possible that such decisions may be motivated by political considerations providing a false sense of security to the population. Operating without clear and fact based standards by which to make assessments that "guarantee a level of security" will chill investments not just in cyber security technologies and solutions but in all manner of business decisions including mergers, acquisitions and product launches as all these decisions have a cyber security component. Moreover, enforcement measures taken after an event and against an ill-defined scale will only create confusion and uncertainty.
3. Market operators and public administrations will provide mandatory notification of any incidents that have a 'significant impact' on its core services. However, there is no clear guidance on what sort of incidents trigger mandatory notification. This requirement largely mimics an earlier US Securities and Exchange Commission guidance, which has been met with substantial confusion, poor compliance and has not generated any

evidence that it has improved security. Moreover, as discussed earlier, requirement such as this can create significant unintended consequences such as stock manipulation

4. Member States will undertake a significantly enhanced oversight role in the investigation of non-compliant entities, security audits and the issue of binding instructions to market operators. The lack of clarity as to what significantly enhanced oversight will mean in any particular case will lead investors to fear the worst and invest the least. Cyber investments are already complicated and expensive. EU entities wishing to maintained competitiveness may well need to adopt new technologies such as cloud based services, long international supply chains, Bring Your Own Device to Work and other business practices that require substantial investment but could undermine security . Not knowing if such investments will pass this intensified oversight will have a chilling effect both on investment, innovation and productivity. Moreover, this concern is not confined just to cyber information systems. All manner of contemporary business decisions now have a cyber security component and lack of certainty will affect these also with potentially negative effects for job creation and growth.
5. Member States should adopt "effective, proportionate and dissuasive" sanctions for non-compliance. Exactly what this means and how such sanctions will be reconciled between states is unclear. Companies doing business in the EU, including those currently located here, will likely make future business decisions based on the risk these ill-defined sanctions may take on their bottom line. This undermines the goal of stimulating business growth in the EU --- again without any evidence that this measure will enhance security. Moreover this is the essence of the blame the victim mentality that reflects a naive and fundamentally flawed understanding of modern cyber threats.

Finally, compounding the uncertainty is the simultaneous reform of EU Data Protection laws. While the draft NIS Directive and Data Protection reform are separate initiatives, there will be a significant overlap between security and breach notifications. The overlap will inevitably lead to confusion, and uncertainty will inevitably subject the private sector to even more conflicting demands and costs again undermining economic growth without enhancing security..

ISAFE, a coalition of major EU based enterprises from multiple economic sectors and diverse national base strongly urge the EU Commission to rethink their approach to the cyber security directive and reform it to create a coordinated world based system that appreciates the uniqueness of the 21st century cyber threat and adopts a collaborative "social contract model"

INTERNET SECURITY ALLIANCE FOR EUROPE

[i] McAfee and the Center for Strategic and International Studies. "The Economic Impact of Cybercrime and Cyber Espionage." Rep. *McAfee.com.* McAfee. July 2013. Web. 31 Mar. 2014. <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf>.

[ii] Exec. Order No. 13636, 78 Fed. Reg. 11739-11744 (Feb. 19, 2013). Web. 1 Oct. 2014. <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

[iii] Internet Security Alliance. "The Advanced Persistent Threat." Rep. ISAlliance.org. Internet Security Alliance, 2013. 1 Oct. 2014. <http://www.isalliance.org/isapublications/>.

[iv] Help Net Security. "Cybersecurity Concerns Becoming a Boardroom Issue." *Net-security.org*. N.p., 06 Mar. 2014. Web. 21 Apr. 2014. <http://www.net-security.org/secworld.php?id=16482>.

[v] Ponemon Institute and HP Enterprise Security. "2014 Cost of Cyber Crime Study: Germany". Rep. *hp.com.* Ponemon. October 2014. Web. 27 Oct. 2014 < https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5211dede.pdf>

[vi] Ponemon Institute and HP Enterprise Security. "2014 Cost of Cyber Crime Study: United Kingdom". Rep. *hp.com.* Ponemon. October 2014. Web. 27 Oct. 2014 < https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5209enw.pdf>

[vii] Ponemon Institute IT Security Tracking Study Estimates, Feb. 2012

[viii] Internet Security Alliance. "The Advanced Persistent Threat." Rep. ISAlliance.org. Internet Security Alliance, 2013. Oct. 2014. <http://www.isalliance.org/isapublications/>.

[ix] Kopan, Tal. "FEINSTEIN: GOVERNMENTS 'KNOW' ABOUT HACKING:." Politicopro.com. Politico PRO, 28 Oct. 2014. Web. Oct. 2014. <https://www.politicopro.com/cybersecurity/whiteboard/?wbid=42778&print>.

[x] Geers, Kenneth, Darian Kindlund, Ned Moran, and Rob Rachwald. WORLD WAR C : Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks. Rep. N.p.: FireEye, n.d. Print.

[xi] Hewitt, John D., and Marie-Helen Maras. *Exploring Criminal Justice: The Essentials*. By Robert M. Regoli. Burlington, MA: Jones & Bartlett Learning, 2013. 378. Print.

[xii] Perera, Dave. "NIST: CONFIDENCE NOT COMPLIANCE IS C-WORD IN CYBERSECURITY FRAMEWORK." Politicopro.com. Politico Pro, 30 Oct. 2014. Web. 31 Oct. 2014. <https://www.politicopro.com/cybersecurity/whiteboard/?wbid=42938&print>.

[xiii] Nesterov, Vladimir. "The Financial Perils of the Eurozone." Global Research. Strategic Cultural Foundation, 23 June 2014. Web. Oct. 2014.

[xiv] Peter C. Evans and Marco Annunziata, Industrial Internet: Pushing the Boundaries of Minds and Machines, General Electric, 13 (November 26, 2012).

[xv] Swedish Agency For Growth Policy Analysis. "The Economic Effects of the Regulatory Burden." (n.d.): n. pag. Ec.europa.eu. Swedish Agency for Growth Policy Analysis, Dec. 2010. Web. Oct. 2014.

[xvi] Dreher, Axel, and Martin Gassebner. "Greasing the Wheels? The Impact of Regulations and Corruption on Firm Entry." Public Choice 155.3-4 (2013): 413-32. Web. Oct. 2014. <http://download.springer.com/static/pdf/549/art%253A10.1007%252Fs11127-011-9871-2.pdf?auth66=1414683718_3e18609ae7dbaec0a9efdfaa8c8f022f&ext=.pdf>.

[xvii] Merle, Matthew, Raju Sarma, Tashfeen Ahmed, and Christopher Pencavel. "The Impact of E.U. Internet Privacy Regulations on Early-Stage Investment A Quantitative Study." (n.d.): n. pag. Http://www.strategyand.pwc.com/. Booz & Co. Web. Oct. 2014. <http://www.strategyand.pwc.com/media/uploads/Strategyand-Impact-EU-Internet-Privacy-Regulations-Early-Stage-Investment.pdf>.

[xviii] Internet Security Alliance. "The Cyber Security Social Contract." Rep. ISAlliance.org. Internet Security Alliance, 2013. 1 Oct. 2014. <http://www.isalliance.org/isapublications/>.

[xix] Ibid

[xx] Obama Administration "Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure". May 2009. Oct. 2014.

[xxi] Exec. Order No. 13636, 78 Fed. Reg. 11739-11744 (Feb. 19, 2013). Web. 1 Oct. 2014. <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.
[xxii] National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0." Framework, 12 Oct. 2014. Web. <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.
[xxiii] Exec. Order No. 13636, 78 Fed. Reg. 11739-11744 (Feb. 19, 2013). Web. 1 Oct. 2014. <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.
[xxiv] Mitchell, Charlie. "Government's Emphasis on Private-sector Leadership Seeks to Ease Regulatory Concerns." Login. Inside Cybersecurity, 29 Sept. 2014. Web. Oct. 2014. <http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/governments-emphasis-on-private-sector-leadership-seeks-to-ease-regulatory-concerns/menu-id-1075.html?s=dn>.
[xxv] Mitchel, Charlie. "FCC Official: Industry Comments Will Shape Policy, Not Regulations." InsideCybersecurity.com. Inside Cybersecurity, 30 Sept. 2014. Web. Oct. 2014.
[xxvi] Inside Cybersecurity. "Commerce Official Says Use of Cyber Framework Lends Liability Protection." Insidecybersecurity.com. Inside Cybersecurity, 3 Oct. 2014. Web. Oct. 2014.
[xxvii] Inside Cybersecurity. "Utility Groups Promote Expanded Use of DOE Cyber Guidance." Insidecybersecurity.com. Inside Cybersecurity, Sept. 26. Web. Oct. 2014. <http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/utility-groups-promote-expanded-use-of-doe-cyber-guidance/menu-id-1075.html>.
[xxviii] Bernhart Walker, Molly. "White House Won't Pursue Single, Large Cybersecurity Bill." FierceGovernmentIT. Fierce Government IT, 13 Oct. 2014. Web. Oct. 2014. <http://www.fiercegovernmentit.com/story/white-house-wont-pursue-single-large-cybersecurity-bill/2014-10-13>.