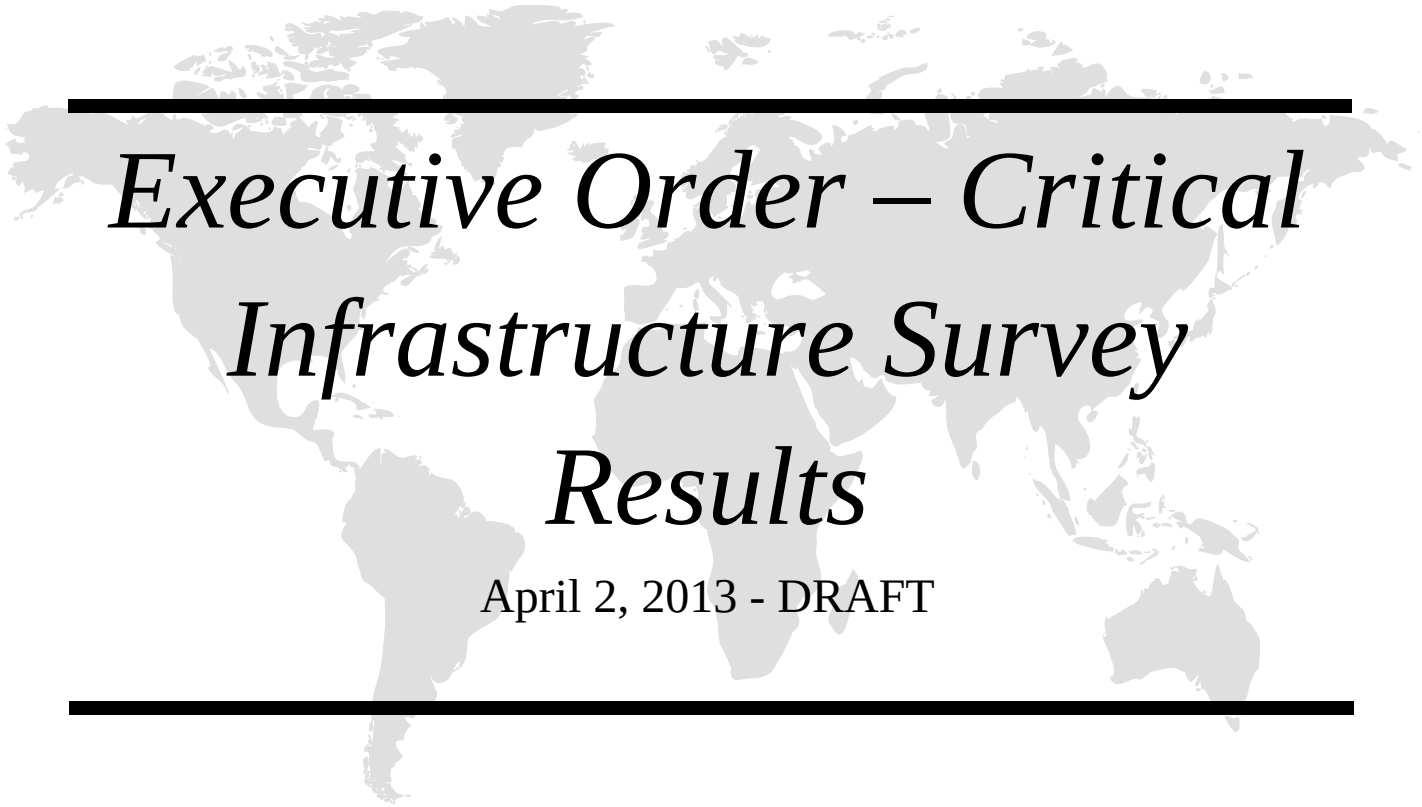

Executive Order – Critical Infrastructure Survey Results

April 2, 2013 - DRAFT

CSA Executive Order – Critical Infrastructure Survey Results

On February 12, 2013, the President of the United States issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity.

The purpose of this survey is to collect a broad spectrum of CSA member opinions to provide feedback to NIST's issued Request for Information, "Developing a Framework To Improve Critical Infrastructure Cybersecurity", Docket Number 130208119–3119–01.

CSA received 30 survey responses in the 2 weeks this survey was open.

QUESTIONS

1. Region of respondent

USA (23)
Canada (4)
Sweden (2)
Italy (1)

2. According to PDD-63, "critical" infrastructures were "those physical and cyber-based systems essential to the minimum operations of the economy and government." In 2013, what if anything would you recommend to enhance the definition of critical infrastructure?

No enhancement 23

Recommended enhancements (7 respondents, USA unless otherwise noted):

1. (Canada) Other dependent systems, one problem with most complex systems (especially infrastructure) is that there may be a critical dependency that we are not aware of and fail to protect/harden so if something happens it still all tips over still.

2. It might be beneficial to clarify 'minimum operations'.

3. (Italy) We agree with the definition of critical infrastructure as "an essential asset for the maintenance of vital societal functions. Damage to the critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have negative consequences for the security , the well-being and the quality of live of the citizens. (rif. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm) Seeing the importance the use of internet has reached nowadays in our life, the protection of citizens in cyberspace has become vital and therefore the protection of critical infrastructure extends to their digital identity and its reputation on the social network.

4. Essential to the minimum operations of healthcare, communications, economy and government.

5. … and where the abrupt failure or misuse of those systems is reasonable to result in unacceptable harm to individuals, or external relationships governments and their economies. **"Abrupt" takes into account the positive expediency automated systems provide, but recognizes the known lack of equal investments in risk mitigating monitoring and response controls, to recover enough from such failures.** **Discussing external governments, takes into account that economically - large internal errors and misuse can quickly cross "interfaces" (consider - misconverting currencies, pulling large/multiple wires in milli-seconds from other markets, and intentional fraud originating on a government system) harming government economies and millions of people internally and externally faster than it can currently be detected now on Wall Street. We still don't know what happened during a 12 second 8 point drop from over 3 years ago on the stock market. So it is in everyone's best interest to expect and ensure failsafes exist to protect our neighbors from fires that originated in our home, which are possible, plausible, and likely.** **"Reasonable" means an investment in controls adequate to be responsible, that participants and neighbors will not incur significant harm from higher speed, frequency, and distances possible from error or malice from our own systems. Controls adequate enough to show that a root cause origination capability exists and can be demonstrated to work quickly enough to adequately stop problems before they grow to large. And, that allows for mutual accountability internally and across such interfaces. The measure of reasonable might be the acceptable restoration costs for our oversights to balance risk taking and prudence. (Keep in mind, there are some situations too large to be able to collect insurance on.)** **We also know now, that there are basic legal business problems that technologies have not addresses to correspond with tried and true business transactions. But, mutual respect requires technology that provides good faith accountability, trusting partnerships, and justice. The test on this - is remuneration possible, if a hacker in Japan steals a citizens' or corporate entities officer identity from our government-held personal information, drains our bank, retirement, and treasury accounts, puts the deposits temporarily in Iceland - will they have any hint of the potential for justice? Commitment to a few failsafes to prevent having no justice? Maybe - demonstration of faithful ways to trace the transactions to an accountable owner to attempt justice or recovery? Internal systems mismanagement with interfaces on the internet are a challenge now. What risk are we willing to bear for harming external parties who can suffer from errors in our own mismanaging our own system, when it results in an offset that starves another county's financial system?** A lot of people don't appreciate that it's not all IT fun and internet games - until their accounts and country's future stolen - with no clue how it disappeared or where it went so fast. :)

6. (Canada) Critical Infrastructure is fairly well defined. What does need attention is the definition of "Critical Information Infrastructure" - i.e. the ICT systems that are essential to operations of physical CI. CII is not really a separate sector but rather is an aspect of all other sectors.

7. Perhaps classified by sic or naics code.

3. Ranking of Critical Infrastructure Sectors

Sector	CI Rating Average (4.0 most critical)
Water supply	3.87
Information and communications	3.80
Electric power	3.67
Emergency law enforcement services	3.47
Emergency fire service	3.47
Banking and finance	3.40
Oil and gas production and storage	3.33
Public health services	3.27
Highways (including trucking)	3.20
Pipelines	3.20
Mass transit	2.87
Rail	2.87
Aviation	2.80
Waterborne commerce	2.67
Continuity of government services	2.67

Potential missing sectors:

- Software vendors
- Justice
- Agriculture
- Food distribution

4. If you are located outside of the United States and your country adheres to a definition of critical information sectors different than the United States, please list the sectors

Italy:

- Agriculture, food production and distribution sector
- Security services (police, military) sector
- National monuments & museum sector
- Media service sector

Canada:

- Health
- Food
- Finance
- Water
- Information and Communication Technology

- Safety
- Energy and utilities
- Manufacturing
- Government
- Transportation

5. Cybersecurity information sharing with the private sector is a key critical infrastructure protection issue. Please provide your opinion on the issues and potential solutions, including existing information sharing frameworks and processes that you believe should be examined for this purpose.

1. Historically government wants availability to information but hasn't been good at sharing relevant information back to the info sec community. Where this has occurred we feel it has been substantially beneficial to both sides. We have our own community with information available at https://atlas.arbor.net which worldwide ISP's and CERTs rely upon for information critical to the health of their networks. We do participate in many trust groups and readily exchange pertinent information to those that have a positive use case. We are willing to work with governments even if that means clearance requirements to obtain and exchange information that would help in the defense of critical infrastructure.

2. The Open Source world has a number of mechanisms for sharing data, mostly email based, they seem to work quite well. I think a major component of this is having trusted relationships between individuals at the various vendors/companies/etc, you can officially do many things but it's the one to one relationships that often allow the really scary stuff to be shared

3. I am extremely interested in the work or initiative being proposed by the people at SecurityStarfish - http://www.securitystarfish.com/index.html. Issues on the subject of sharing include – Protecting customer privacy as well as the companies, contracts that constrain what can be shared, legal repercussions, regulatory repercussions, disparities in information shared in different places to different entities, could the data be subpoenaed, Patriot Act, Freedom of Information, can the release of a little information be used as reasonable cause to request or require the release of more information.

4. Key challenges for the sharing: - Volume of information - Providing information, not just data - Consistent "language" for information (e.g common definitions and understanding of risks, etc) - Timeliness of information - Costs of using information (e.g doing something from actionable intelligence) - Legal issues with NOT doing anything with the information (e.g having received it but not actioning it). May promote some organizations to not participate in knowledge sharing. - Potential issues with information flowing trans border / issues with regulatory regimes and data protection regimes in other jurisdictions (potentially - depending on the type of information involved).

5. We agree that information sharing with the private sector is a key issue as regards critical infrastructure protection. Industry can give an important contribution to improve cyber security. It's role is to work together with government to develop the right policy framework to enhance cyber security. Industry can actively cooperate and collaborate in information sharing and in the formulation of policies in all fields of cybercrime. In particular the most important contribution can be in:
    a. Producing periodical country reports to share information about security incident occurred and the level of damages raised.

b. Defining security measures for emerging threats; in this contest the IT industry should continually innovate and invest in the development of its products and services. Being an innovative and dynamic sector with rapidly changing technologies, the industry can give an important value to the cyber security in addressing new and evolving threats.
c. Collaborating to the development of globally accepted cyber security standards, best practices, and international assurance programs.
d. Developing and utilizing a comprehensive risk management strategies and best practices to achieve and maintain trust in the cyber infrastructure.
e. Cooperating with national and international CERT in incident handling by sharing policies and coordinating the response in case of cyber-attacks which can affect critical infrastructures. Regarding this issue, we suggest examining the guidelines provided by ENISA on the 'Setting up a CERT' http://www.enisa.europa.eu/activities/cert/support/guide."

6. Currently, the FBI generally only want private sector to share. They do not share what they have well (often fairly past-dated). The NSA are even more closed mouthed. The best sharing going on, IMHO, are the security research labs, who have repeatedly discovered and then disseminated vital information about attack types and patterns in a disciplined and rigorous manner. This state of affairs seems really lopsided. It's almost become nation-states watched by global security companies. Huh? Think about flame or Chinese attacks, etc (not to pick on any particular nation-state, the USA included). who's doing the work? A more ideal situation would be MUTUAL sharing. Certainly NIST's CWE/CVE are vital. But these are reactive, not pro-active. We must get to the tip of the iceberg, not the tail underwater, long after the damage has been done. Finally, much has been written about vulnerable critical systems and the huge attack surface these present. If the government wants to actually do something here, it should take the form both of active incentives and probably, fines, as well. Why? the power grid vulnerability, essential services vulnerability, for years. And nothing happens because there is no business incentive to take action. Plus, the risks are unproven (and hopefully will never be if we take action)

7. Until transparency and accountability capabilities are demonstrated to address fairness and safety in our own private transaction markets (dark pools, banks managing multi-tiered private and public mutual funds, high volumes of unknown trading activity without timely checks in private company NYSE for a "public market") to the extent they are already internationalized, and we can demonstrate some intelligence and get serious about efficient oversight systems implementation so HUMANS can oversee critical activities and interact real-time - we are kidding ourselves if we think we can apply the same sloppy management to any critical infrastructure without large consequences.

8. Models exist around the world to address many aspects of public-private information sharing including public-private partnerships, joint exercises, information sharing and alerting networks, sectoral information exchanges, etc. All of these mechanisms have a place in a holistic information sharing approach. The main challenges with information sharing between the public and private sector revolve around security clearances, adversarial approach to regulation, and more general trust issues. Security clearances are usually an obstacle when they are required to share information with a broad set of private sector stakeholders. Most effective approaches seem to combine classified and non-classified information sharing with different audiences - with heavy emphasis on the latter. Private sector hesitation in sharing information with the public side is often caused by fear of regulatory repercussions and/or increased level of regulation. Some of the Scandinavian countries seem to have adopted a different, more collaborative approach to regulation that seems to alleviate some of these issues.

9. The US Federal government, especially the FBI has a well deserved reputation for taking information, but not providing any. This perception and practice has to change. Recommend a mechanism (InfraGard) be used to vet individuals who can then be trusted conduits for information. These individuals may need training on how to Sanitize some intelligence.

10. As information sharing continues to move into the cloud and mobile devices, I'm proposing the framework should include the security structure and elements, including cryptography, of Blackberry.

11. In speaking with peers it seems that the support of UK, the Center for the Protection of National Infrastructure provides information, personnel and physical security advice to the businesses and this is the path to success particularly regarding "Domestic Infrastructure"

6. Which key technology areas are currently high priorities to be implemented to protect Critical Infrastructure?

1. Artificial Intelligence Cryptography Massively Parallel General Purpose Computing Algorithms Nano-scale Materials Composite Materials Quantum Communications Quantum Computing Energy Transmission Methodologies

2. Access and authorization controls, security logging, monitoring AND event correlation

3. Risk assessment tool, to define a framework to evaluate the potential negative impacts caused by security threats and vulnerabilities to critical infrastr. The focus is to ensure availability, reliability and security of networks and systems. GRC tool, since the continuous monitoring is essential to ensure an efficient level of security tools, strategies and policies and to address compliance and risk issue of critical infrastructures. Data Encryption, to address both security and privacy of the data data at rest, in motion and during the elaboration (depending on specific context). Mobile security technologies, which are relevant for the security of both personal data and business information. SIEM and Big data. SIEM is crucial for a Security Operating Center in prevention of cyber incidents, during incident handling and during post incident analysis. SIEM analysis can be related to big data because of high volume of data to elaborate security real time analysis. Identity and Access Management are important to limit and control the access to sensitive data and to critical components of infrastructure like SCADA (control systems of smart grid, nuclear power plants, etc) Cloud security: security issues depend on service model (IaaS, PaaS, SaaS). Security tools should protect the virtualization layer and the hypervisor in addition to the other components. Business continuity system, like secure protocols, redundancy, synchronization tools, traffic balancing. Security measures at network level, like IDS, IPS, DDoS identification and mitigation systems.

4. Web firewalls have held a great deal of promise which has not been realized. (and my company makes one - I'm speaking for myself, not my employer - please don't quote me). Since a great deal of infra is on the 'net, a killer, effective, easy to implement web firewall would help to solve the huge technology debt in this area. No one has (IMHO) cracked this problem. and for sure, attempting to work off the tech debt through coding security, while laudable is obviously not working and won't - there is simply too much deployed vulnerable code. Deep packet inspection has also held a lot of promise that is unfulfilled. This might help to protect critical systems (not web) that are vulnerable. Several have tried (work on a few myself). It's harder than it looks.

5. Identity and accountability systems. The private sector is trying to figure out how to make business work while managing 1000 keys that no IT manager is taking the time to understand and design prudently. The government is trying to figure out how to outsource private financial data while maintaining HIPPA, while finding an access control system for appropriate public participation and protection that isn't a joke - that interfaces well with a 3 factor government employee high-security access control structure. Even the automated systems being built to "predict" for verification of what a user actually has access to internally are confused - so we don't have what we need to do something similar for external parties and international parties yet. We need more investments in joint problem solving for ID and accountability. The current problem is that too much effort is spent on learning about what people are doing now. Documenting what people are doing now, is like writing a biography - it is interesting 0 but it doesn't propell us forward with solutions to shared, known problems. I recently saw a chart of compliant Certificate Authority validation internet traffic. It is obvious that Germany's IT managers and CA's get it - and have something good going on for the basis of a trusted accountabilty plan. If we want international trading of cyberinfrastructure - there needs to be some reason to trust there are mechanisms in place to safely identify and protect individuals. We need technology that supports basic fair business law concepts that have worked for ions. And - the risk of doing busines with the person you don't know - is very high. Look at the escalating credit card identity theft problem - and that's just 1 type of eCommerce transaction.

6. 1) SCADA 2) Mobile 3) "Big Data" and cloud

7. Encryption and enhanced User Activity Review process.

8. Secure internet protocols, Analysis Technologies, Modeling of cyber attacks, Better Threat detection (IDS), Analytically techniques to mine "Big Data" for security purposes.

7. Privacy and Civil Liberties Protections. What are the key risks to citizen rights from an increased focus on cybersecurity protection of critical infrastructure and how do we achieve the appropriate balance?

1. Well we already have warrantless wire tapping and Internet surveillance and FISA so I'm pretty sure we already crossed that bridge without realizing it.

2. In a cloud environment, the data does not or may not belong to the cloud provider, by which I mean, the CSP is entrusted with data, not necessarily given data, to do with what ever the CSP wants, ie the Data Subject (DS) – and what the DS was told his data would be used for… will the CSP be able to share DS data if it is outside of what the DS was told the data was used for… and how does this data and its lifecycle expire? (age of data, or the DS ceases to be a customer or user and wants their data expunged) Once it is shared… will that data remain forever? If data is shared, and if through means of multiple sources of information, a DS is implicated in a larger issue related to illegal or terrorist acts… how will that implicate or obligate the CSP?

3. Limitations on speech and information access. Prosecution or detention without due process

4. "It's hard to find a right balance between privacy and national security, freedom and need of control. There is no a right answer, but there is a clear risk of sacrificing privacy and freedom. When it comes to privacy, each country reflects the orientation of its legal and political system. In USA privacy is defined

as “the right to be left alone”, while in Italy it has a wider meaning and includes “the right to self-determination” (ie religious freedom) and “individual sovereignty"". The Italian privacy law is very stringent. It’s contained in Legislative Decree of 30 June 2003, n. 196, named Personal Data Protection Code. On January 25 2012, the European Commission adopted a regulation on the protection of personal data, which adds definitions of new types of data (ie biometric data); introduces the principle of EU law also to the processing of personal data carried out not in the EU, whether related to supply of goods or services to EU citizens or such as to enable the monitoring of the behavior of EU citizens; establishes the right of citizen to ""data portability"" but also the ""right to be forgotten"", and so on In Italy TLC providers must also respect:

a. prohibition of listening, tapping and storage of communications of individuals without their consent
b. obligation to interception request from judicial authority
c. obligation to erase or make anonymous personal data related to billing and to process such data only for the period of time strictly necessary (6 months). Italian authority is also working to implement the Directive 2009/136/EC related to cookies."

5. CISPAA, inspecting every citizen's financing and online communications MUST STOP IMMEDIATELY! These are unconstitutional and unnecessary. Spying isn't the way to solve these problems. Let's focus on what needs to be protected. The Internet is a grand experiment in a global commons. It is very democratizing and that has been generally a Good Thing. Still, democracy is a noisy, mob ruled mess. that's the nature of the beast. If we want Arab Spring, we have to have Wikileaks and Occupy, too. (no matter you politics) The Internet will be key to solving many of human kind's major issues, take climate change or hunger, AIDS, what-have-you. In order to preserve this commons, people need to feel some sense of entitlement and safety. But like any commons, others will always try to exploit the situation (hence any number of malefactors trying to hurt others via the Internet). Protection of privacy will be critical to continuing success. There is no other way Ultimately, the items listed above breech the very fabric of society. How can we speak of privacy in the face of the USA government's (or any government’s) inspecting every online activity? The balance is to follow the US constitution's protections in an online, digital manner. That does NOT mean looking at everything and everyone just because we can. It means focused investigation for a purpose.
Without privacy and choice, there is no freedom. Someone had the bright profitmaking corporate motive 15 years ago, and decided the US was a default "opt-in country unless declared otherwise". We'd have a basic personal privacy stance to start with if that didn't happen, if .gov didn't already give it away. People are more likely to think that you are a criminal trying to hide, than respect that a prudent private citizen who questions coughing up all personal information on demand. The government needs to do a needs requirement assessment, and build a solution that meets those needs. Some of these problems are so muddled, that we probably need a public vote on what we want and a discussion of why - before we can build a technology that supports it. I'm all for privacy - but the lack of forethought makes it so we have unnecessary denied services - instead of a well-designed system that supports a right to privacy. Maybe Obama can have a town meeting where we vote live for different nuances? It needs to be thought out. Right now - we have a "give up you privacy, or give up your other rights" policy. For example: - My $8000 homebuyer tax credit took 9 months, I was accused of fraud, and had to get help from the new taxpayer advocacy service, because they said I couldn't live in a PO box and I decided not to register my physical address. Seriously. The effort to resolve it increased the IRS' handling costs 10 fold. - I can't see if my Social Security salary balances are correct. My online ID application information was sent to Equifax to ID me. Equifax is unable to answer whether or not I am who I say I am, due to a privacy protection freeze on my account. It would keep the risk footprint smaller by using an internal data search with info the government already has on me. A scan of my Federally issued passport, info from my last tax return, where I was born, Etc. There are ways of protecting the right of

privacy - we just can't give in because corporate players say there is no other solution (they who want another income source and more unnecessary public spending).

6. Personal information protection and privacy needs to be defined for electronic systems in a way that balances personal freedom with effective law enforcement. The privacy vs surveillance debate has been fairly hot recently, but the balance has not been yet attained. FISA (Foreign Intelligence Surveillance Act) seems to be getting increased attention while the Patriot Act continues to raise fears about privacy and data protection from US based service providers. Incidentally, anonymity should not be considered an integral issue alongside privacy. Privacy and data protection can be achieved without anonymity; in many cases lack of anonymity plays a role of a deterrent.

7. Due process and 'unreasonable' suspicion are challenges. Racial/Religious profiling while politically unpopular has been shown to be a component of security.

8. The privacy law in Massachusetts serves as a good example for what constitutes breach notifications. At a minimum, California SB1298 and SB1386 should become nationalized.

9. The Patriot Act of 2001 I would submit as a success of excess... It is a vital tool and I say should be an example of success rather than a risk to citizens rights.

8. What critical infrastructure is at greatest risk from a cybersecurity incident of catastrophic proportions and why?

1. Power, water, and nuclear. Obviously these systems are core to modern human living and survival and it is well proven that these systems are rife with vulnerabilities and access controls that put them at risk.

2. SCADA. SCADA software as a rule is terrible and wide open. My biggest concern would be physical damage to high value/hard to replace infrastructure like power plants, the good news is most things are hard to break so unless you're handling dangerous materials/fuel/etc the worst that can (hopefully) happen is an unclean shutdown.

3. Water systems – as a means to propagate disease/viral infections. Water management is an issue because it is so vast. You cannot simply stop needing water and you cannot go very many days without a source of clean water. Communication systems – it's the pathway to all other systems, financial, power, managing complex systems for rail, aviation, government. Compromised communication causes huge hurt almost instantly. At issue is that it has become so complex and so diverse – the threat surface is enormous.

4. All monitoring and decision-making (statistical analysis, etc.) systems, especially of the "Big Data" variety. The greatest risk may well be specific data corruption rather than wholesale deletion.

5. Those infrastructure pieces that cannot revert to manually controlled or minimum service levels. For instance highways and certain mass transit systems can still operate safely even if systems are compromised. For instance mass transit could degrade to have a limited number of trains on the track/switch to bus traffic, etc. Services like Air Traffic Control can not degrade service quickly or safely. Also those infrastructure services where minimal human interaction is involved or the infrastructure is highly distributed and automated (e.g pipelines, telecoms grids, etc).

6. "One of the most critical sector could be the transport sector (eg. flights, trains, etc.) whose management, scheduling, control etc.. is computerized: for this reason a cyber-security attack could cause serious incidents due to the number of deaths and the block trade. Even the TLC systems are vital infrastructure: an attack on the backbone, for example, could make unavailable all connections based on the backbone which implement the services to support all other critical infrastructure. The energy production systems can be even more critical, because an attack could not only cause blocks of production, with serious damage to the state country, but also put out of use the infrastructure of TLC support to all the others. Other high priority sectors are those relating to Defense and Emergency: the latter is particularly at risk because it is involved in extraordinary situations not easily predictable. For all sectors it is generally true that become more critical the higher is the risk exposure. Another important area is healthcare since some aspects can affect a very big population:
    a. mistakes and failures can lead to personal injury which can reach up to the death of patients (safety
    b. in many contexts, the emergency is not an exception: slowing down of activity, perhaps due to authorization processes in access to information, are not acceptable;
    c. the issue of security and the protection of personal data have strong overlap, as the most critical data are included among those defined as sensitive by the regulations."

7. Water and electricity. These vulnerable systems are well known. It's time, as I wrote, above, to incentivize protections, and perhaps dis-incentivize inaction. Let's deal with the known first. We have tremendous technology debt in this arena, e.g., we are very vulnerable. Let's protect those systems first so that people can live in the event of either cyber war or armed conflict or both.

8. Investment-related banking. High impact. High fraud self-benefit. Low transparency. Quietly done fast. There are many more smart technology students internationally, than decent security controls. Generally - The Fed's support systems. I would say more - but I would rather not create a specific security target.

9. Finance and banking are critical this is a sector that is constructed upon trust, and has gown to be a pillar of our way of modern life. If this infrastructure and the trust would be compromised that would render to a catastrophe.

10. Information and Communication and its dependencies including Finance, SCADA systems underlying transportation and energy, as well as systems that support health, law enforcement, fire, etc.

11. Agriculture and health care. Security is not a concern - of course SCADA bound elements such as water and power are at risk, but these are much more well known.

12. The power grid has the largest potential for creating massive disruption.

13. Electrical grid, water supply, food supply - these are must haves! Banking would be next on my list

9. Which voluntary activities can the private sector better execute upon to improve cybersecurity

1. The number one activity that would allow for greater defense is an exchange of information to those that are actively involved in the defense of critical infrastructure. While this is easier said than done the

conversations that occur between public and private sector are far more productive than relying on the private sector taking this challenge upon themselves only.

2. Write software that doesn't suck so bad.

3. Cyber threat and event sharing would be beneficial, if we can determine how to do so. Making the investment to learn and require their company to adopt Cyber Security Best Practices and then developing actual Best Methods (A best practices might say "Don't store confidential data in a log file", the company then must develop a 'Method' that is practical to meet the requirements of the Practice) Secondly, the private sector needs to INSIST that the academic organizations (colleges/universities) do a better job of training Software Developers, DBA's, Network Engineers, System Administrators and such on cyber security, not just on the specific science.

4. Security of all stored information Security of communications Preventative measures against identity theft

5. Define and follow minimum baseline standards on an industry by industry basis.

6. Cooperation with private sectors (such as universities, industries, associations, ISP, etc.) and government institutions is important to raise awareness to the cyber security issue and to ensure the resilience of critical infrastructure and the availability of the services. This cooperation can be more effective if it involves also international partners. Prevention is fundamental to contrast the cybercrime and cyber-attacks. Governments can promote the institution of Computer Emergency Response Teams (CERT) and encourage the involvements of private corporations for information sharing, education strategies and response coordination. Private sector can offer skill, professionality, knowledge and tools to enhance the resilience of critical information infrastructure. The aims of this collaboration could be:
    a. Defining security measures for emerging threats;
    b. Elaborating a kind of "template" of cyber-security strategy and policy (from a super-parties entity like ENISA or others) to be adopted as a reference model.
    c. Providing web sites to sharing information about cyber-security incidents and new threats or exploits;
    d. Measure the efficiency of tools and policies, and share and compare the results.
    e. Promoting security awareness and training activities related to security management.
    f. Promoting the sharing of security services and tools (each sector for its competence, for example a TLC provider could provide network security network tools to protect the communication component of critical infrastructure or DDoS detection/mitigation services).

7. Somehow, patching systems has to become a priority. It is well known (certainly by the makers and readers of this survey) that it's unpatched but fixed vulnerability that is taken advantage of most frequently. the high profile, clever attack is very rare. Let's make that the only thing we have to worry about, rather than failing miserably at table stakes activities like grunt patching.

8. Not allowing the trade exchanges (like NYSE and NASDAQ) to allow the buyers of IT trading pipes to resell IT access and redistribute to unvetted legal parties. Require registration and trust certifications of software developers. Separate business equipment from personal IT toys. i.e., no default social media frameworks on my work BlackBerry - and don't make unsigned, untested software available to download to the phones. Cloud providers should be required test what happens when connecting clouds - like what happens to an IT admin's BlackBerry when agreeing to BlackBerry's Cloud Services through MS 365. It's not all about software guys.... Small financial institutions need to get together and

require an independent privacy audit of Intuits' use of data collected via QuickBooks and Digital Insight's infrastructure support of small credit unions and banks.. Along those lines - what crazy person thought it was a good idea to make the worst-secured, high-volume consumer technology - web-enabled phones - to do consumer SMS payments between bank accounts? Where is the OCC? The Fed? FFIEC? FTC? ???

9. 1) Implementing rigorous CII risk assessment and preparedness 2) Continuous collaborative sharing of best practices and threat intelligence 3) Proactive public-sector information sharing
10. Government has to show these activities won't be prosecuted and that the government is will to be a true partner.

11. Begin moving towards a better User Authentication process. Stop using common 2 factor authentication based on passwords.

12. Command and control and interoperability between government and private sector. Other nations are seeing a mutual sharing and responsibility with government to protect its "electronic borders"

10. FOR CRITICAL INFRASTRUCTURE SECTOR STAKEHOLDERS: In your system security plan how do you categorize criticality of systems and address protection, stability and recovery of these assets based upon the defined criticality?

1. We categorize the criticality of systems mainly based on the following matters: business impact; number of customers; legal obligation (ie lawful interception requirements, privacy law, laws specific to application sector, like banking/financial, etc); social and government requirements (ie for the health of the users, rescue, etc). Depending on the criticality of the system we identify and implement specific security measures. For example if the system requires stability and availability, we perform a strict monitoring and design a robust recovery strategy (like backup, redundancy, geographically distributed, etc). When there is a legal obligation we have to put in place all the security measures to guarantee the respect of these laws (for example in terms of control access, data encryption, and so on).

2. 1) Will it kill people? 2) Can a lot of people get really personally harmed? If so, plan to minimize the likelihood of either 1 and 2 happening BEFORE using it; and a plan to fix it fast before it does hurt, in case it happens anyway without intention. That's called Management. Specifically, Risk Management. Most people think more about getting more access and toys; and turn a blind eye to knowing the consequences. We can't expect a better internet for students, business, or government, by continuing to allow technologies where the errors of a few can affect masses of people quickly (insert link-based bot-virus here), and continue to trust the end points to decide well for the community on whether they should install any cute little phone app.

3. Security should be approached from both inward and outward facing systems simultaneously until meeting in the middleware infrastructure components.

11. FOR CRITICAL INFRASTRUCTURE SECTOR STAKEHOLDERS: Would a strongly protected, highly anonymous, reporting system for incidents be acceptable as a method for information sharing?

1. YES but it is not always required.

2. Yes - except apparently CPA firms who audit outsourced IT services and are trying to develop secure cloud artifact solutions for accountability auditing, aren't considered an important enough conduit. So we don't "qualify" to participate and advise our clients on what's hot to protect .... though we are all about educational communication for risk management with our clients ..... Writing up IT security issues is not fun nor good for business. Education is much more future-valuable.

3. Anonymous sources are not always reliable. While some sources may need or want protection, validation of the source is more important to insure the intelligence is accurate and reliable. Anonymous systems may be used by our enemies as well as those with good intentions. Diversions can be as effective as attacks.

4. Yes, similar to SANS at a minimum but with more detail in terms of where the attacks are originating, what ports are being used successfully and unsuccessfully.

12. FOR CRITICAL INFRASTRUCTURE SECTOR STAKEHOLDERS: Who within your organization holds direct responsibility for the system security plan – for creation, execution and reporting responsibility?

1. Within our organization there is a function at Corporate level which has the responsibility to define the high level security policies and procedures for the company (ie privacy compliance and other regulations of interest in each regions). At regional level there are local risk management functions which have the responsibility to elaborate the system security plans, in conformance to the policy and procedures defined at Corporate level. The risk management functions cooperate with the regional Security Operation Centers for the executions and reporting of security operations.

2. Stakeholder: Those who would be harmed if critical infrastructure failed. That's the public. I think you mean the question to be "For those who support a critical infrastructure organization".

3. Me - and my small business is certainly critical to my infrastructure.

4. CISO

13. How do you see key CSA research areas (Cloud, Mobile, Big Data) impacting Critical Infrastructure over the next 5 years?

1. The threat landscape follows the infrastructure. As we introduce and roll out new types of infrastructure such as cloud and mobile, and come to rely on these infrastructures more and more as a party of daily business and life the more critical they become. Cloud represents a visibility and lack of control in terms of expanding networks beyond the borders of traditional IT networks. Mobile is now becoming core to every day communication and productivity and is a natural extension of network infrastructure

traditionally supplied by providers. Essentially these infrastructures are the transport mechanisms of many of the critical infrastructure items mentioned earlier in the document.

2. Cloud will be one obvious thing, a lot of stuff that shouldn't be moved to the cloud probably will be (my sister works at a SCADA firm, the executives wanted to put SCADA stuff “into the cloud”, never mind the remote sites barely had dialup).

3. The CSA will be a leader in the thought process first as a means of developing best practices and methods, and second, it will be a powerful force to drive those practices and methods into actual practice by the private and public sectors. The CSA serves a significant role in the field of research, both government and university, as the means for the private sector to have a voice in the research process. Private industry is interested in this subject and how it will be addressed, managed and policed, but unless they are one of a few very large companies, they have few options for representation. The CSA uniquely provides that type of representation. I think that CSA research will improve Critical Infrastructure security.

4. Increasingly important as guidance as more critical services start to leverage, or provide data to, cloud based services.

5. The use of mobile devices by citizens is becoming increasingly common in order to access services and applications. Mobile devices can be also used for online banking and financial applications and now also for m-commerce. The infrastructure components of ICT sector become more exposed to risk, due to the diffusion of mobile devices and their low security level. This lack of security, together with business reasons, makes these devices an attractive target by attackers. Cloud model is emerging also in Italy: the progressive computerization of the public sector, a critical infrastructure, and the fact that the choice to implement public services often falls on cloud model mean that critical infrastructures are increasingly based on the cloud (e.g. Public health and Governmental services). The Italian Digital Agenda promotes the use of cloud computing and also the Ministry of Defence believes that having cloud based services is useful to limit costs and get flexibility. For all these reasons cloud security issues are relevant in order to preserve security of critical infrastructures. The extraordinary growing of user data, traffic data, and data from monitoring tools makes the ability to manage Big Data an enabler for achieving effective security. On the other hand, many sectors of critical infrastructure are based on big data: a typical example of big data producer is the backbone of a TLC provider, that is also a critical infrastructure. This is why is doubly important to elaborate statistical models and data mining techniques to identify new security symptoms and threats.

6. Big Data mostly. Because both finding and protecting vulnerability is a big data problem. But also, finding, understanding, and protecting against new attack patterns is also a big data problem

7. If the past serves as a model: 1) corporate for-profit interests and IT security people will continue to drown out efforts needed on the crucial ID trust, accountability, and governance management artifact retention architecture needs in CSA forums; 2) NIST's resources will be taken off course again from making a public benefit difference, by pressure from #1 into another year of unnecessary dancing to cross-reference/map more CSA and other pro-provider standards changes, further slowing down any progress on decent SLA, IT business accountability, and verification practices (even though business laws already address them just fine now). The providers do a good job promoting CSA. Unfortunately, CSA is also being used as a tool to prolong accountability. There will never be a perfect standard for any business. The frameworks need to be molded appropriately for contracts, laws, and the

specific risks of delivering a particular service - cloud or non-cloud. We need less thinking, and more DOING on the security front.

8. All of the CSA research areas are already and will increasingly impact CI. Mobile is becoming a key part of the ICT CII today while commercial interests are pushing Cloud and Big Data to become part of various CIs in the near future.

9. This is the new front line in cybersecurity.