Commission on Enhancing National Cybersecurity

Established by Executive Order 13718,
Commission on Enhancing National Cybersecurity

U.S. Department of Commerce - Commerce Research Library
Herbert C. Hoover Building, 15th and Pennsylvania Avenue NW, Washington, DC

MEETING MINUTES

The Commission on Enhancing National Cybersecurity was convened for its first meeting at 1:00 P.M. Eastern Time on April 14, 2016 at the U.S. Department of Commerce, Washington, DC. The meeting in its entirety was open to the public. For a list of meeting participants, please see Annex A.

Opening of the Meeting / Introduction of the Secretary of Commerce

Kiersten Todt, Executive Director of the Commission on Enhancing National Cybersecurity, NIST

Ms. Todt called the meeting to order and introduced the United States Secretary of Commerce Penny Pritzker. As the 38th Secretary of Commerce, Secretary Pritzker, has made cybersecurity the focus of her efforts and of her agencies since she was sworn in three years ago. She understands the need to make risk management a priority in both the public and private sector. She has overseen one of the most significant achievements of the administration on cybersecurity, the development of the NIST Voluntary Framework for improving critical infrastructure cybersecurity.

Welcome

Penny Pritzker, U.S. Secretary of Commerce

Introductory Remarks and Commissioner Introduction

Secretary Pritzker thanked Ms. Todt for the introduction and welcomed everyone to the Department of Commerce and the first official meeting of the commission. She noted the work of this commission is the core of the Cybersecurity National Action Plan. The commission has been charged with presenting a forward-thinking cybersecurity report that diagnoses the greatest vulnerabilities facing government, business, and consumers, in today's digital economy; and to make actionable recommendations that should be taken for the next decade by the private sector and every level of government, and serve as a roadmap for continually strengthening US economic and national security, supporting the development of technological solutions and best practices and empowering the American people to guard their identities and assets while online.

The President's vision for the commission involved bringing in twelve of the brightest minds in business, academia, technology, and security. Secretary Pritzker thanked and acknowledged the chair and vice chair of the commission for their expertise in the national security arena and business. She noted the Department of Commerce is uniquely positioned to support the efforts of this commission. Commerce engages daily with industry and government in efforts to secure the nation's financial assets, intellectual property, personal data, and network infrastructure. The private sector is critical to the Department of Commerce, as well as to this commission, as they are

the owners and operators of much of the nation's critical infrastructure and digital networks, the backbone of the 21st century economy.

It was noted that the NIST already is a leader in the cybersecurity field. NIST developed the cybersecurity framework as a common language of risk management for IT experts and non-experts. The National Cybersecurity Center of Excellence (NCCoE) was established as a public/private research partnership to develop technical solutions that are adaptable for organizations of every size and every kind. Additionally, the National Initiative for Cybersecurity Education (NICE), a public/private sector initiative, was created to develop workforce skills for cybersecurity and to support employers as they look to hire, train, and re-train staff on cybersecurity.

The Department of Commerce and NIST are here to help and leverage any resources available to assist with the commission's work. The Department of Commerce looks forward to supporting and partnering with the commission in the months ahead, as the commissioners assist the nation in securing its future.

Introductory Remarks and Commissioner Introduction

Thomas E. Donilon, Commission Chair, O'Melveny & Myers, Vice Chair, Former U.S. National Security Advisor to President Obama

Samuel J. Palmisano, Commission Vice Chair, Retired Chairman and CEO, IBM Corporation

Mr. Donilon thanked Secretary Pritzker for her work and leadership in the cybersecurity field, and welcomed the commissioners. Mr. Donilon expressed gratitude for the assistance received from Commerce and NIST, and to the commissioners for accepting their roles. Mr. Donilon brings the perspective of a former national security advisor. Cybersecurity is a challenge to the government and citizenry. He noted that cybersecurity technology has been named the leading threat to the country by the Director of National Intelligence James Clapper, for the third time in his world-wide threat assessment. We currently have increased exposure to attacks in security and the economy, An enormous volume of devices are coming online, and the threat is growing.

Mr. Donilon noted that the work of this commission is well-timed to give a detailed set of recommendations for actions that can be taken over the next five to ten years. The report is due to the President on December 1, 2016. Given that timing and the upcoming election, the commission's report will effectively serve as a transition memo to the next President. The question to be asked is, if the commission were to sit down with the next President, what are the most important things that can be done to protect the country from threats posed by cybersecurity. President Obama indicated that if during the course of the commission's workthere are immediate steps that the commission believes the President should take before he leaves office, he would want to hear them.

The commission is meeting today to accomplish five things:

1. Provide the necessary Federal Advisory Committee Act (FACA) and ethics briefings for the commission, along with introductions of the commissioners.
2. Hear from Lisa Monaco, the Assistant to the President for Homeland Security and Counterterrorism. She will provide her view of the problem, from the perspective of the White House.

3. Allow the commissioners to comment with respect to the scope and priorities of the commission.
4. Plan a timeline for the workshops and meetings.
5. Open the room to thoughts and views from the public.

Samuel J. Palmisano, Commission Vice Chair, Retired Chairman and CEO, IBM Corporation

Mr. Palmisano added his additional thanks to everyone joining the commission and providing their time and effort for the commission. The internet today is dramatically different from its defense origins. Businesses are impacted by security and privacy, and those that don't evolve get left behind.

From a business perspective, the internet now touches everyone in their personal lives. We are currently only at the early stages of this digital technological revolution and it's only going to expand. Therefore, everyone's focus on technology adoption rates is likely bound to the security and privacy of the internet; therefore, policies that can protect both companies and individuals need to be developed. It is not only a current problem; it will be more prevalent in the future.

Commissioner Introductions:

Pat Gallagher – Currently Chancellor at the University of Pittsburgh; formerly the Director of NIST;
Heather Murren – Former commissioner on the Financial Crisis Inquiry Commission, prior to that the founder and CEO of a cancer treatment center, and prior to that approximately a decade on Wall Street;
Steve Chabinsky – General Council and Chief Risk Officer of CrowdStrike, previously with FBI cyber division;
Herb Lin – Senior Research Scholar for cyber policy and security at Stanford University;
Joseph Sullivan – Chief Security Officer at Uber; former Chief Security Officer of Facebook;
Peter Lee – Microsoft Research Corporate Vice President;
Annie Anton – Professor and Chair of Interactive Computing at the Georgia Institute of Technology;
Keith Alexander – Founder/CEO of IronNet; former Director of the NSA; retired four-star General US Army; former Commander U.S. Cyber Command.

There were two commissioners that could not be in attendance for this meeting:

Ajay Banga, President and CEO of MasterCard;
Maggie Wilderotter, Executive Chairman of Frontier Communications.

Ethics Briefing and FACA Briefing

Gaye Williams, Department of Commerce, Office of the General Counsel, Deputy Chief, Ethics Law and Programs Division

Ms. Williams, Deputy Chief of the Ethics Law and Programs Division, was joined by Mr. DJ Spence, an attorney in the Ethics Law and Programs Division, to share a brief explanation on the ethics briefing. This briefing takes place in five steps:

1. The commissioners must review the top 10 ethics rules for special government employees serving on advisory committees, provided by Ms. Williams. The contact information for the Office of the General Councel is listed on the bottom of the outer envelope and on the pen

provided with the package. She noted her contact information is listed at the top of the envelope provided to the commissioners, and her staff is available to support the commissioners while serving on the commission.

2. The second piece of information is the handout, the top 10 ethic rules. These are the rules that apply to the commissioners in their capacities as special government employees serving on advisory committees. These rules only apply when acting in the official capacity on this commission. They do not apply to outside work, such as the routine jobs held by the commissioners. The impact from the rules should be minimal as this only applies to the commission's work. Commissioners with questions should not hesitate to call Ms. Williams's office.
3. Inside the envelope is a copy of the financial disclosure report submitted by commissioners to the White House along with the application/nomination to be a part of this commission. The office reviewed the information provided, pre-cleared it for its completion, and verified the information reported does not conflict with the work of this commission. A conflict of interest waiver is also included. The report needs to be signed and dated (as long as the information is still correct and valid), and returned today. A draft waiver is included to ensure that nothing commissioners do on this commission that could potentially affect their financial interest.
4. A copy of the waiver will be sent electronically once they are made available. One-on-one briefings or group briefings are available if more appropriate. The Office of General Counsel can be on the agenda of the next meeting if necessary.
5. Please contact the Office of General Counsel if there are any question and Ms. Williams will be around for the first part of this meeting if there are any questions that come about from this briefing.

Alice McKenna, Department of Commerce, Office of the General Counsel, Senior Counsel

Ms. McKenna is an attorney for the Office of the General Counsel who has specialized in the FACA for the past 25 years. She gave a brief introduction to the FACA, with the understanding some may be familiar with it if they have served on other advisory committees. FACA is an open government statute passed in 1972. FACA is very similar to the Freedom of Information Act as both have an emphasis on openness and transparency in government operations.

FACA governs what federal agencies do, not what individuals do. While the ethics office engages with the commissioners personally, the office's FACA clients are NIST as an agency, and the officials within NIST. FACA requirements impact how the government interacts with the commission and how the government is obliged to hold meetings and interact with the public to satisfy the act's openness and transparency requirements.

FACA requirements include:

1. A presumption that the meetings will be opened to the public.
2. The public will be provided at least three weeks' advance notice of these meetings in the Federal Register.

3. All meeting minutes, transcripts, or any documentary materials, regardless of form or format, that have been provided to, for, or by the committee (statute language) are available to the public upon request.

Typically, a three week lead time is required to schedule a notice for publication in the Federal Register. Questions can be routed through the commission to Ms. McKenna.

Commission Scope of Work Discussion (Part 1)

Commissioners of the Commission on Enhancing National Cybersecurity

Mr. Donilon began the scope of work discussion. One of the principal goals of the meeting today is to have the commissioners talk about their views on the scope and priorities of the commission, and to build out the commission work plan. The executive order provides eight broad topic areas for the commission to study and come up with recommendations, along with providing the commission a broad opportunity to expand on the topics that it wants to discuss. There is an authority to order original research, and conduct public workshops around the country. The eight topic areas that are outlined in the executive order are:

1. **Federal Governance,** with respect to procurement, management practices for Federal IT civilians, Federal workforce cyber hygiene practices, and Federal legacy systems. The goal is having the federal government become a model for practices and technologies in cybersecurity.
2. **Critical Infrastructure**, with respect to promoting effective private sector and government cooperation and approaches to infrastructure within cybersecurity.
3. **Cyber Workforce,** in both the private and government sector. At a national level, there has been a market failure in this arena. But we now have an opportunity to expand on what is being done at a smaller scale by federal government in institutions as well as in state and local governments. To come up with a single initiative on cyber workforce has been a real need, but we do not currently have the supply of properly trained talent to fit this goal. There are different challenges to the private and government sectors, and working on this will enhance the quality/quantity of workforce for both.
4. **Internet of Things**, referring to new technologies entering the cyber environment. There are currently billions of new devices connected and we have the opportunity to get out in front of this trend, with respect to security and privacy concerns.
5. **Research and Development**, the President is looking to the commission for the research and development goals for the next decade. Where would we allocate resources and the kinds of technologies and practices we need to look into going forward?
6. **Public Awareness and Education,** the cyber hygiene practices of the users of the new devices. In 2014, IBM reported that over 95% of cybersecurity incidents involved human error or stale practices still being used.
7. **State and Local Government,** cooperation in enhancing cybersecurity. The Governor of Virginia stated that cyber will be the number one priority of his term as the head of the National Governors Association (NGA), and we will be working closely with him and others

around the country with respect to how federal, state, and local governments can enhance cybersecurity.

8. **Data and Identity Theft Protection,** including all the systems and data and identity management and the security of online identities.

The executive order also explicitly directs us to include other things that we think are important within this commission's work. We should also consider the issues of insurance and making a stronger stance in the international realm going forward, with a strong emphasis on deterrence and developing international norms by working with countries who are willing to work on this topic.

Mr. Sullivan pointed out that we have an issue today with companies seeing government involvement with cybersecurity issues only in response mode after something bad has happened, to either help catch the threat or to levy sanctions on companies for not being good enough. We never see the government laying the foundation of the "safe road" for companies, as NIST is trying to accomplish now. Could we be the "New Deal" for the internet and technology by identifying the practices that should be foundational to good security on the internet? Could we use this budget to have the government practices be a model? Currently, the government is not a model, but a laughing stock; the commission can use this opportunity to turn that perception around.

Mr. Donilon noted that the federal government is the biggest purchaser of technology in the country and we have the ability to drive practices. We also have the horizon with this executive order to drill down hard on these points. Mr. Palmisano said we likely need to establish a global standard that everyone can comply with for cybersecurity practices and data protection.

In other industries, such as vehicles and transportation, there is a strong emphasis put into the prevention of catastrophic events, such as forcing the automobile industry to adopt seatbelts and airbags, and pushing for speed limits, etc. There does not seem to be anything like this being done in the technological realm at this time.

White House Briefing

Lisa Monaco, White House, Assistant to the President for Homeland Security and Counterterrorism

Ms. Monaco comes with the approach of trying to lay out the problem from the perspective of the White House along with the charge that the President has put forward with this executive order. The commissioners were strategically selected to provide an array of perspectives that will be critical for the success of this commission.

Why is the commission necessary? In short, the commission is needed because we are more connected now than we have ever been before. For decades, the innovation and growth of technology and the internet has been a strategic advantage for the United States. If we don't tackle the fundamental issues with cybersecurity threats that we face, we risk having that strategic advantage become a vulnerability and a liability. To tackle this task, we need a commitment that transcends political ideology and cuts across private and public entities, a commitment that can draw together concrete recommendations that will outline the strategic vision for the future.

The administration has been focusing on these issues from the start, since 2009, and it has taken a number of steps, such as raising international defenses, improving our incident response, and other

similar efforts. The Cybersecurity National Action Plan, established in February 2016, is the capstone of the administration's two terms. It provides near-term and long-term components and actions to be taken.

The challenges we face cut across several dimensions. The firstis security, both national security and homeland security. The hostile actors in this sphere are more diverse, more capable, and getting better at what they do, and the attack vectors they operate against are increasing. There were 1 billion connected devices in 2009; today there are approximately 6.5 billion, with projections that the number will increase to 20 billion by the year 2020. We have so many devices now entering the digital realm, and so many diverse actors, that the challenge of security is very high and the barriers for hostile actors are very low. Moreover, it is often difficult even to attribute a particular attack or security-related event to a particular hostile actor.

Ms. Monaco noted that the second challenge we face is policy. From the policy perspective, cybersecurity is a source of major risk to government and business. How we think of those risks and how we then think of addressing them are just beginning to grow. There are too few metrics to assist us in understanding what is going on. From a governance perspective, there are legacy systems, and siloes within systems, as well as a culture of bureaucratic stasis. There are few incentives relating to cybersecurity, even though there are enterprise-level risks if cybersecurity measures are not taken. Risk management relating to cybersecurity must be elevated beyond IT departments.

The third problem is technology and systems architecture. Security has not been a primary factor in innovation. The commission needs to consider how systems should be designed and built from a security perspective.

The fourth problem in this realm is the broad issue of consumer behavior and privacy. In short, how do we protect and verify identities online? There must be a move beyond the password. Society understands cybersecurity threats in the abstract, but the government must take the lead in taking steps to show people how to protect themselves concretely.

The commission has a national agenda. Its work will lay the foundation for the next administration and for the next decade. The audience for the commission must be society as a whole, not merely the federal government. Recommendations must be actionable and address the root challenges we face. The Cabinet will be available to assist the commission with its work. For all the areas to be covered by the commission, good ideas already exist that can be expanded upon. The IT modernization fund, NICE, a multi-factor awareness campaign, and initiatives to reduce the use of social security numbers are among the existing government initiatives that can be considered by the commissioners.

Mr. Donilon acknowledged Ms. Monaco's extensive background in national security and thanked her for the briefing. He then opened the floor to the commissioners for questions.

Mr. Lin: What is different now than any of the efforts that have taken place in the past?

Ms. Monaco: The government has taken more steps to make progress than has been done in the past, though none qualify as a silver bullet. Examining legacy systems, and fundamentally rethinking cybersecurity governance involves getting outside of entrenched approaches, and

looking for new strategies. The government has acquired a greater degree of knowledge and experience. It hopes to use these experiences to make a difference now.

Mr. Lee: Are there processes in place to keep up with the evolution of threats?

Ms. Monaco: We do not expect this commission to come up with one technology recommendation that will solve this issue. There is no crystal ball, but we can examine trends (*e.g.*, biometrics) and seek to discern what the real solutions are. The commission has the capability to look ahead.

Mr. Palmisano: Why, in your experience, is it hard to get things done?

Ms. Monaco: Sometimes it takes a set of diverse minds without particular interests to find solutions to problems. Interest in the status quo can prevent progress.

Mr. Sullivan: Why is it important for the commission to be partnered with Commerce?

Ms. Monaco: There has been a lot of good experience in the past, happening mainly in the NIST framework process. Having stakeholders with various perspectives is important for developing solutions. That lesson, learned while developing the framework, is applicable to the commission's effort.

Companies often don't talk to the government until something bad happens. Who in the government is responsible for creating the right environment for businesses to collaborate prior to events? There needs to be more and diverse channels for businesses to share information with the government. Private sector companies should have relationships with government agencies. Learning from private sector experiences will be helpful across the board.

Ms. Anton noted for many years, the US has not negotiated with terrorists. Ransomware has been the recent exception to the policy. The government does not practice the policy of non-negotiation with terrorists where ransomware is concerned. Ransomware incidents are gaining attention now, as they are on the increase. There is tension between the two schools of thought on negotiating or not negotiating with terrorists. There may not be enough data yet to determine who is employing ransomware. There needs to be more intelligence analysis to determine sources and causes.

Mr. Donilon: What does the President have in mind when thinking of empowering citizens with respect to cybersecurity?

Ms. Monaco: It relates to the norms question. People generally accept the idea they must do something to protect themselves when engaging in particular activities (such as driving and wearing seat belts). The goal is to make it commonplace for people to do certain activities to protect themselves when engaging in internet activities. The norms the commission will help develop will have an impact in this area. The commission audience truly covers everyone from individual consumers to large organizations.

Commission Scope of Work Discussion (Part 2)

Commissioners of the Commission on Enhancing National Cybersecurity

The commission has the ability/opportunity to drive practices. We know practices need to be improved. There are short and long term practices that need to be considered. Instituting better practices would take care of a large number of threats.

Mr. Lee: There are two thought processes, involving the near term and where might we be in ten years. The commission may not be able to do both.

There needs to be a pipeline for security engineers. There is a market failure in the private sector that the commission may be able to address: Mr. Sullivan pointed out that there is a 20% premium on security engineers in Silicon Valley, suggesting a shortage the market has failed to address. Strong academic tracks for cybersecurity need to be created. The NSA has developed some academic "centers of excellence" to develop tracks in cyber security. Even though security engineers are in high demand, there still are large numbers of open positions.

Ms. Murren observed that one important observable phenomenon the commission should note is that anxiety has been increasing in American households, in particular due to health insurer incidents. Many Americans are looking for a greater understanding of how to increase their security.

Mr. Chabinsky noted that the challenge for the commission is to not have the fourth in a line of documents that just sit there. The challenge is to look into the work that has been completed, and the recommendations that have been provided previously so that we are not repeating history. Documents have been sent to Ms. Todt on this issue. The challenge for the commissioners is not to reproduce what's already been done on all the topics discussed. Recommendation to the group to look at previous efforts and see what's gone right, wrong, etc.

Many initiatives over the years get broken down into too many components, making them too challenging to work. Complexity is an issue to be considered by the commission. The cybersecurity problem has become so large that only the largest organizations may be able to do something to help themselves. It is counter-intuitive that a small organization or individual may have a more challenging time achieving cybersecurity than a larger organization with many parts and legacy systems.

There is a great need for real metrics. Metrics remain an unsolved problem in computer science after 40 years. There have been no really good metrics for cybersecurity, and if this commission can come up with some good metrics, it should publish them in computer science journals. Mr. Lin noted his concern about history repeating itself. Defining metrics has been a long term challenge.

Mr. Lin also observed that, based on his experience recently leaving the government to work in Silicon Valley, public-private partnerships need help. Many private sector business managers perceive the government as the enemy. Some senior managers in IT companies tend to regard the government on a level of distrust comparable to how China is regarded.

General Alexander agreed that government can't do it alone. The commission must present options that involve the private sector. Working with industry is only part of the problem; international relationships must work too. Setting standards is very difficult. The US must reach out to other governments to encourage working relationships on standards. Insurance companies set standards for coverages. The commission should also consider insurance impacts.

The percentage of automated tasks versus the percentage of manual tasks may be off. The probability of human error needs to be reduced dramatically. The commission should consider how to take humans out of the loop where possible, and reduce the percentage of errors. He noted what

the space program did in the sixties led to everything we have today. How can the commission have a similar impact?

Mr. Gallagher said the challenge in cybersecurity is fundamentally different than anything that has come before. Past practice may simply not apply any more. The commission may need to examine where mistakes are repeated and why. The expectation that we can manage human behavior may be incorrect. Where have continuous calls for improvement not worked? It may be worthwhile to examine these areas.

Mr. Lee observed that future deterrence may lie in data dominance. The culture in Silicon Valley is different in that it encourages experimentation and learning by trying. It fosters growth, agility, and evolution by avoiding aversion to risk. The government is at a transition point with regard to its mindset. It is worth noting that the cultural difference is due to younger people having a different perception of the world. Echoing the same concern, Mr. Palmisano noted that government is perceived by most young innovators as an inhibitor of progress. The interest to protect the past is viewed as an inhibitor to progress. Neither side is listening to each other at present. At some point there needs to be a resolution. Norms cannot developed without Silicon Valley being involved. The only way to get a consensus is for both sides to work together to arrive at cybersecurity norms.

Ms. Anton asked what it would mean for the nation to respond to a major infrastructure attack. There were fundamental breakdowns in protocols, systems and technologies during the 9/11 attacks. There was no ability to focus on more than one plane or first responder communications. How can we ensure that scenario is not repeated in future incidents?

Much needs to be done on transparency. What is privacy in the context of the internet of things? Trust is crucial; there is a fundamental distrust of government and government systems. It is difficult to define privacy when everything is being collected. There is no knowledge of what's being collected, who sees it, and there is no way to opt out.

The new administration will need a comprehensive look at cyber. Deterioration of the relationship between government and companies is severe. There are new things happening, and there are real vulnerabilities. Can technology assist with dealing with human failings? Can we avoid the failure of imagination that happened before 9/11?

Mr. Donilon suggested a change of mindset may be needed in many areas. Good ideas also need to be reinforced. The timing for change is favorable with a new administration coming in. The deterioration of the relationship between the government and private companies is a side effect of the Snowden incident. Threats are changing and new vulnerabilities are being discovered. Will technology enable us to address fundamental failings that are rooted in human frailty? It becomes crucially important to think imaginatively. Can we imagine what we would do the day after a major event?

We have the opportunity to be pre-emptive and proactive in our actions now. Technologies exist that make it difficult to make mistakes. People, processes, and technology becomes a theme for people to have better choices in situations where the potential to make a mistake exists.

Ms. Todt pointed out that it may be worthwhile to examine the 9/11 and financial sector crisis commissions to see why things occurred and what may have been prevented if proper authorities

were given to people who needed it. We need to examine why we fail to act on known vulnerabilities.

How does government share with industry? There is no way for industry to talk to government about cybersecurity. The underlying problem is how to enable government to get information in a way that is not concerning to companies (no PII). Both sides of the government-industry story may not be shown. How can the government publish the good work it does? If perceptions of the government are not corrected, little progress will be made. General Alexander suggested the government plays a role as a sort of fire department for cybersecurity fires. The government must be able to stop terrorist attacks and protect the citizenry. There are measures the government can put forward to create positive perceptions. Measures must be agreed to by everyone, and processes must be transparent. Currently, there is no "9-1-1" for cybersecurity.

Intellectual property is being lost, and private wealth is being lost. In absolute terms, it represents the greatest loss of wealth in history. So far, the loss has been deemed acceptable. The feeling is a significant event will have to occur before real change happens. Mr. Chabinsky suggested partnership needs to focus less on information sharing as an end in itself, and more on collaboration. The objective for collaborating must determine the action sharing. The commission needs to consider what the barriers to sharing are.

Mr. Sullivan stated that there is a need to consider consistency as well as complexity. There is no consistent procedure among judicial districts regarding whether hospitals should pay to get their information back in response to ransomware threats. Why does the industry call government after a cybersecurity event? And perhaps more importantly, who can people call before an event happens for preventive measures? For example, whose job is it to get to prevention on ransomware? There is no answer to these questions now.

Mr. Lin asked what incentives have we or should we set up to incentivize the private sector to collaborate with the government. Collaboration may mean businesses may expect greater transparency in the process, and possibly more concrete results of collaboration (technologies, or other tangible benefits). There may need to be independent oversight to uphold transparency. It has been true in the past, that companies may assist the government, but then have no further participation in the process. There is some expectation, on the side of companies, that some more tangible return for the information is expected. In areas where extensive civil liberties and privacy concerns exist, it may be worthwhile to set up oversight bodies so that there is public insight that the correct processes are being followed.

As the commission works, it must define its scope of work. We will need to define all these issues with the same intensity, and what bucket they will ultimately belong in.

Mr. Donilon observed that if a product has a vulnerability, it is important to avoid a knee-jerk reaction and impose regulation. A better response might be to develop standards that will protect users. Are there private sector mechanisms to deliver standards (UL, formerly Underwriters Labs) that might be used to further the process? Standards can range from being soft to much more rigorous. Most safety standards are voluntary in this country. The right incentives must exist for companies to follow standards.

The commission may want to consider some fundamental principles and possible choices relating

to those principles. What principles may be applicable to standards? Labelling standards for these types of products should be looked at, so people can understand what products do. There are two types of standards: what things do, and standards to keep things from happening.

Ms. Anton and Mr. Gallagher pointed out that throughout the history of the internet, investments by government in universities have created new industries. The commission is to think about basic R&D and investment priorities for the next administration. More than 2/3 of R&D is done by industry. The government should examine how it can work with industry on what it's doing. How can it work so that everyone benefits?

The Chair's framework for the commission's work is a great start. Distributing the framework to the commission will help develop things further. Groups of commissioners will also be focusing on specific areas. Education must be considered on multiple levels. It's not just technical, but it's everyone "knowing what to do." Leadership issues exist in that cybersecurity must compete with other priorities. An awareness exists now with executives about hygiene vs revenue issues. It has now reached the board level. The Commission hopes to create a culture of security.

The workforce problem is bigger than just the specialists the leadership needs to be educated and take “heed” to the issues with cyber security within government and agencies.

Review of Commission Timeline

The best way to solicit input from the public and private sectors is to conduct workshops around the US. Dates for workshops have been proposed to the commissioners. The commissioners will review the workshop dates. The Commissioners should attend most if not all.

The first workshop will be in May, in New York City; the second, in June in San Francisco, CA; the third in July, in Houston, TX; the fourth in August, in the Midwest - Minneapolis, MN, or Chicago, IL; the fifth in Washington, DC.

The commission will hold two types of meetings, public workshops and commission deliberation meetings. A scope document needs to be developed soon, followed by a detailed scope document with the final recommendation topics. Three deliberation meetings will be scheduled in the fall. Deliberations will use technology as a means to share information. The contact list will be distributed after the meeting.

Public Comment

Mr. Don O'Neill spoke to the commission on resilience in the face of cybersecurity incidents. The government and the NIST NCCoE may be setting the bar too low. Government can do more than withstanding, controlling damage, and recovering from adversities, either man made or natural. This approach is limited in that it does not account for actions to prevent the cascading triggers that result. Anticipation and avoidance measures must be a part of the government's plan. The commission should hold the government's feet to the fire for the greatest possible result, including anticipation and avoidance. A paper with Mr. O'Neill's statements was provided to Mr. Kevin Stine of NIST, and will be distributed to the commissioners.

Meeting Adjourned

Meeting adjourned at 3:45 P.M. Eastern Time.

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Kiersten Todt
Executive Director
Commission on Enhancing National Cybersecurity
NIST

Tom Donilon
Chairman
Commission on Enhancing National Cybersecurity

These minutes will be formally considered by the Commission at its June 2016 meeting, and any corrections or notations will be incorporated in the minutes of that meeting.

ANNEX A – List of Participants

Last Name	First Name	Affiliation	Role
Todt	Kiersten	NIST	Executive Director, Commission on Enhancing National Cybersecurity
Donilon	Thomas, E.	O'Melveny & Myers, Vice Chair, Former U.S. National Security Advisor to President Obama	Commission Chair
Palmisano	Samuel, J.	Retired Chairman and CEO, IBM Corporation	Commission Vice Chair
Alexander	Keith	Founder/CEO of IronNet, Former Director of the National Security Administration, and retired four-star general who headed U.S. Cybercommand	Commissioner
Anton	Annie	Professor and Chair of Interactive Computing at the Georgia Institute of Technology	Commissioner
Chabinsky	Steve	General Council and Chief Risk Officer, CrowdStrike	Commissioner
Gallagher	Pat	Chancellor, University of Pittsburgh	Commissioner
Lee	Peter	Microsoft Research Corporate Vice President	Commissioner
Lin	Herb	Senior Research Scholar, Stanford University	Commissioner
Murren	Heather	Former commissioner on the Financial Crisis Inquiry Commission	Commissioner
Sullivan	Joseph	Chief Security Officer at Uber	Commissioner

Last Name	First Name	Affiliation	Role
McKenna	Alice	Department of Commerce, Office of the General Counsel, Senior Counsel	Presenter
Monaco	Lisa	White House, Assistant to the President for Homeland Security and Counterterrorism	Presenter
Pritzker	Penny	US Secretary of Commerce	Presenter
Williams	Gaye	Department of Commerce, Office of the General Counsel, Deputy Chief, Ethics Law and Programs Division	Presenter
O'Neill	Don	Don O'Neill Consulting	Presenter/Public Participation
Chalpin	JP	Exeter Government Services	Meeting Staff
Cook	Melanie	NIST	Meeting Staff
Drake	Robin	Exeter Government Services	Meeting Staff
Salisbury	Warren	Exeter Government Services	Meeting Staff
Artz	Sharla	SEL, Inc.	Attendee
Border	William	not given	Attendee
Brewer	Tanya	NIST	Attendee
Bush	Megan	American Trucking Associates	Attendee
Castellin	Chris	PWC	Attendee
Clark, III	Major	SBA Advocacy	Attendee
Cotto	Tony	NAIC	Attendee
Cressey	R.	LGV	Attendee
Crimando	Stephen	A.P.I.	Attendee
Cushing	Chris	NWKS	Attendee
Davidson	Alan	DOC	Attendee
Dillard	Regina	State Farm	Attendee
Dodson	Donna	NIST	Attendee
Douglas	Derek	Deloitte	Attendee
Dwyer	Nick	Delta Risk	Attendee
Egel	Naiomi	CFR	Attendee
Eggen	Matthew	US Chamber	Attendee
Felten	Ed	OSTP	Attendee
Flatgard	B.	NSC	Attendee
Forostia	Michael	SANS	Attendee

Last Name	First Name	Affiliation	Role
Fritts	CJ	US Bank	Attendee
Hairston	Tara	Honda	Attendee
Hanson	Michael	SABRE	Attendee
Harman	Michelle	NIST	Designated Federal Officer, Commission on Enhancing National Cybersecurity
Kane	Daniel, T.	SBA Advocacy	Attendee
Kaul	Krystie	Deloitte	Attendee
Keefe Singer	Jenilee	DOC	Attendee
Kerben	Jason	State	Attendee
Krebs	Chris	MSFT	Attendee
Magri	Josh	FSR/BITS	Attendee
Mayer	Robert	Not legible	Attendee
Mitnick	Drew	Access Now	Attendee
Mohn	Amy	DHS/NPPD	Attendee
Morgan	Sean	Palo Alto Networks	Attendee
Niejelow	Alex	Master Card	Attendee
Pascoe	Cherilyne	Senate Commerce	Attendee
Peterson	Rodney	NIST	Attendee
Pillitteri	Victoria	NIST	Attendee
Prior	Kevin	Williams & Jensen	Attendee
Raigster	Krisha	Bank of America	Attendee
Retske	Alyssa	Lobbyit.com	Attendee
Schlom	Evan	OMM	Attendee
Siegel	Zach	Monument Policy Group	Attendee
Spence	DJ	Department of Commerce	Attendee
Stine	Kevin	NIST	Attendee
Thomas	Amy	Cyber Student	Attendee
Tropolo	Christian	BSA	Attendee
Walker	B.	OMM	Attendee
Walker	Pamela	ITAPS	Attendee
Walsh	Julie	Finn Partners	Attendee
Behr	Peter	Energy Wire	Media
Boyd	Aaron	Federal Times	Media

Last Name	First Name	Affiliation	Role
Cussan	John	Telecom Reports	Media
Goode	Darren	Politico	Media
Lynch	David	Financial Times	Media
Lyngads	Sean	FCW	Media
Merrion	Paul	CQ Roll Call	Media
Mitchell	Charlie	Inside Cybersecurity	Media
Sternstein	Aliya	Govexec.com	Media

Annex B – Statement of Public Participation

Comments Delivered to the Commission on Enhancing National Cyber Security at the Kickoff Meeting on April 14, 2016

When it comes to resilience, the Government, including the NIST Cyber Security Center of Excellence, is setting the bar too low.

For best results, the value proposition for resilience is based on the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity whether natural or man made under all circumstances of use. Instead, the Government is settling for the operations of withstanding, minimizing, and recovering. Why is this a problem?

The most consequential threat to resilience lies in the cascading and propagating triggers that lie hidden in the complexity of critical sector interactions and dependencies inherent in the system of systems that make up the Critical Infrastructure. Without anticipation and avoidance, cascade triggers are left unattended.

For example, the Banking and Finance sector must remain ever vigilant during the trading day for evidence of triggers that might impede next day opening of the market. Here anticipation and avoidance including shutdown are preferred over recovery, cleanup, and delayed market opening in maintaining trust in the Banking and Finance sector.

A recommendation from the Commission to hold Government and Critical Industry's feet to the fire in seeking the best possible and necessary results on resilience including anticipation and avoidance would make all the difference and would strike a blow for freedom for all of us. In the end, it is a matter of will.

I have supplied Kevin Stine of NIST with a written statement on this and have asked him to submit my paper to the Commission in association with the kickoff meeting. Thank you.

1:52 minutes

Don O'Neill
Independent
Consultant Don
O'Neill Consulting
ONeillDon@aol.com

Former President (2005-2008)
Center for National Software
Studies

Report Summary

This research is designed to stimulate and advance the management and measurement of Critical Infrastructure resilience earned value based on convincing evidence. Simply put, the resiliency value proposition is a critical infrastructure capable of anticipating, avoiding, withstanding, minimizing, and recovering from the effects of adversity whether natural or man made under all circumstances of use.

Based on nearly 50 indicators of resilience, resilience earned value analytics employ the most convincing evidence available to measure the degree to which the resilience value proposition is being achieved both collectively and in each industry sector and the degree to which resilience risk continues to persist. All this is based on an architecture of resilience that squarely faces the issues of harmonizing a diverse industry sector culture and context and offers effective prescriptions for success in the form of well trained Intelligent Middlemen, a resiliency maturity framework, a systems of systems technical architecture, a common and useful way of working, and an integration engineering program structure staffed by a capable resilience integrator.

Reference

Jacobson, I., Lawson, H.B. (2015) "*Software Engineering in the Systems Context",* Edited by Ivar Jacobson and Harold "Bud" Lawson, College Publications, Kings College, London, ISBN 978-1-84890-76-6, 2015, 578 pages.

Banking and Finance Sector Cascade Trigger Use Case

The Banking and Finance sector illustrates the stovepipe cultural environment and technological vulnerabilities that stand ready to trigger societal impact. Its institutional dependence on public trust and its operational dependence on electrical and telecom resilience under stress with its tightly coordinated recovery time objectives make it vulnerable (Jacobson, 2015).

In banking and finance, the financial services industry depends on a network of systems that process instruments of monetary value in the form of deposits, loans, funds transfer, savings, and other financial transactions. The network is composed of banks, other depository institutions, and the Federal Reserve System as well as underwriters, brokerages, and mutual funds. In addition there are industry utilities including the New York Stock Exchange (NYSE), the Automated Clearing House (ACH), Depository Trust Clearinghouse Corporation (DTCC), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT) as well as underlying third party electronic processing services (EMP, 2004).

The Interagency Paper (Bank, 2001) pinpoints clearing and settlement systems as the most critical business operations at risk for financial markets and the disruptions of clearing and settlement processes would have an immediate systemic effect on critical financial markets. The use of the term "systemic risk" is based on the international definition of systemic risk in payments and settlement systems (FED et al, 2002).

The Federal Reserve Board specified that the following functions are critical to the operation and liquidity of banks and stability of financial markets and require same day recovery:

- Large–value inter-bank funds transfer, securities transfer, or payment-related services, such as Fedwire, Clearing House Interbank Payments System (CHIPS), Depository Trust Clearinghouse Corporation (DTCC), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT)
- Automated clearinghouse (ACH) operators
- Key clearing and settlement utilities
- Treasury automated auction and processing system
- Large-dollar participants of these systems and utilities

The banking sector depends on maintaining the trust of the banking community and the banking public. In large measure this trust is maintained through the transparency and verification inherent in exchanges. Without this trust the banking system itself risks anarchy. Overall, the stock exchanges and their associated clearinghouses have performed due diligence and taken the steps necessary to

ensure the resilience of their operations.

1. Under what circumstances might the trust in the banking system be tested and stressed? At the close of each business day it is the expectation and practice of the banking community that the banking ledgers of branch offices be reconciled and balanced to the penny and that securities and trading firms create a daily P&L.
2. Under what circumstances of use might the banking ledgers be thrown out of balance impacting the daily closing and settlement process… and the next day opening?
3. More specifically what is the least Cyber Security exploit capable of impacting next day closing?

References:

Bank (2001) *A Glossary of Terms in Payment and Settlement Systems*, Committee on Payment and Settlement Systems, Bank for International Settlements, 2001.

EMP (2004) *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, Volume 1: Executive Report, 2004.

FED et al (2002) *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System,* The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, September 5, 2002.

Jacobson, Ivar and Bud Lawson (2015), *"Software Engineering in the Systems Context",* College Publications, Kings College, UK, ISBN-13: 978-1848901766, October 2015, 578 pages.

Don O'Neill

Don O'Neill is a seasoned software engineering manager and technologist currently serving as an independent consultant. Following his twenty-seven year career with IBM's Federal Systems Division, Mr. O'Neill completed a three-year residency at Carnegie Mellon University's Software Engineering Institute (SEI) under IBM's Technical Academic Career Program and has served as an SEI Visiting Scientist.

As an independent consultant, Mr. O'Neill conducts defined programs for managing strategic software improvement. These include implementing an organizational Software Inspections Process, directing the National Software Quality Experiment, implementing Software Risk Management on the project, conducting the Project Suite Key Process Area Defined Program, conducting Team Innovation Management training, and conducting Global Software Competitiveness Assessments. Each of these programs includes the necessary practitioner and management training. As an expert witness, he provides testimony on the state of the practice in developing and fielding large- scale industrial software and the complex factors that govern their outcome with respect to competitiveness, security, and trustworthiness.

In his IBM career, Mr. O'Neill completed assignments in management, technical performance, and marketing in a broad range of applications including space systems, submarine systems, military command and control systems, communications systems, and management decision support systems. He was awarded IBM's Outstanding Contribution Award three times:

1. Software Development Manager for the Global Positioning (GPS) Ground Segment (500,000 source lines of code) and a team of 70 software engineers within a $150M fixed price program.
2. Manager of the FSD Software Engineering Department responsible for the origination of division software engineering strategies, the preparation of software management and engineering practices, and the coordination of these practices throughout the division's software practitioners and managers.
3. Manager of Data Processing for the Trident Submarine Command and Control System Engineering and Integration Project responsible for architecture selections and software development planning (1.2M source lines of code).

As an inventor, Mr. O'Neill has two patents pending. One, trademark registered Trusted Pipe™, is entitled *"Business Management and Procedures Involving Intelligent Middleman"*, an apparatus and method for the inside track to offshore outsourcing. The other, trademark registered Smart Pipe™, is entitled *"Business Management and Procedures Involving a Smart Pipe of Tiered Innovation Management Teams"*, an apparatus and method for harvesting ideas as intellectual property from knowledge workers on projects, whether onshore or offshore.

Mr. O'Neill served on the Executive Board of the IEEE Software Engineering Technical Committee and as a Distinguished Visitor of the IEEE. He is a founding member of the Washington DC Software Process Improvement Network (SPIN) and the National Software Council (NSC) and served as the President of the Center for National Software Studies (CNSS) from 2005 to 2008. He was a contributing author of "*Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness",* a report on the Second National Software Summit. Mr.
O'Neill has served as a reviewer of National Science Foundation (NSF) software engineering research proposals and has served as a member of the NIST Software Assurance Metrics and Tool Evaluation (SAMATE) Advisory Committee (2006-2008). He has authored Business Case articles for the CERT Build

Security In (BSI) web site. He has lectured on global software competitiveness, innovation, and outsourcing at the National Defense University (NDU) and on Software Risk Management at George Washington University (GWU) and San Diego State University.

His current research is directed at public policy strategies for reconciling privacy and security stresses; deploying resiliency in the nation's critical infrastructure; disruptive game changing fixed price contracting tactics to achieve DOD austerity; smart and trusted tactics and practices in Supply Chain Risk Management Assurance; a defined Software Clean Room Method for transforming a proprietary system into a Clean System devoid of proprietary information, copyrighted material, and trade secrets and confirming, verifying, and validating the results, and a constructive approach to sequencing the transition of SEMAT Essence Kernel Alpha states with an eye to pinpointing the risk triggers that threaten success and lead to the accumulation of technical debt.

Mr. O'Neill is an active speaker on software engineering topics and has numerous publications to his credit. He has a Bachelor of Science degree in mathematics from Dickinson College in Carlisle, Pennsylvania.

® Trusted Pipe is registered with the U.S. Patent and Trademark Office by Don O'Neill.

® Smart Pipe is registered with the U.S. Patent and Trademark Office by Don O'Neill.

http://www.linkedin.com/in/oneilldon

IBM Research Report 2016 27081790

Integration Engineering in the Pursuit of Critical Infrastructure Resilience

The Role of the Resilience Integrator

This research is designed to stimulate and advance the management and measurement of Critical Infrastructure resilience through earned value based on convincing evidence. Simply put, the resiliency value proposition is intended to yield a critical infrastructure capable of anticipating, avoiding, withstanding, minimizing, and recovering from the effects of adversity whether natural or man made under all circumstances of use. Based on nearly 50 indicators of resilience, resilience earned value analytics employ the most convincing evidence available to measure the degree to which the resilience value proposition is being achieved both collectively and in each industry sector and the degree to which unattended resilience risk continues to persist. All this is based on an architecture of resilience that squarely faces the issues of harmonizing a diverse industry sector culture and context and offers effective prescriptions for success in the form of well trained Intelligent Middlemen, a resiliency maturity framework, a system of systems technical architecture, a common and useful way of working, and an integration engineering program structure staffed by a capable resilience integrator.

Outline

Appendix A: Convincing Evidence Of Resiliency Integration
Engineering Appendix B: Pilot Program Definition

Key Words:

integration engineering elements, critical infrastructure resilience, value proposition, architecture of resilience, indicators of resilience, resilience analytics, intelligent middlemen, resiliency maturity framework, system of systems architecture, way of working, resilience integrator, resilience harmonization, formality in architectural framework, strong code management, cascade triggers, product sourcing exposures, supply chain assurance, cyber security strategy, resilience earned value, unattended value, resilience risk calculation, convincing evidence

Abstract

The critical infrastructure is the industrial base on which the competitiveness and security of the nation are dependent. The current state of the nation's critical infrastructure is at risk. The Internet has become the central nervous system of the nation both private and public. The nation's critical infrastructure continues to be vulnerable to natural disasters and cascading Cyber Security attacks (CrossTalk, 2011). In fact, software has become the critical infrastructure within the critical infrastructure as noted by Dr. Alan Salisbury at the Second National Software Summit (NSS2) in 2004 (Jacobson, 2015). It is here in the mashup among an immature software profession (Defense AT&L, 2015), a vulnerable Cyber Security environment, and diverse and interdependent industry sectors that the challenge of system of systems resilience is born.

Recognizing this, the 2016 White House Cyber Security National Action Plan (CNAP) contains a provision entitled, *"Enhance Critical Infrastructure Security and Resilience"*. The Department of Homeland Security, the Department of Commerce, and the Department of Energy are contributing resources and capabilities to establish a National Center for Cyber Security Resilience where companies and sector-wide organizations can test the security of systems in a contained environment, such as, by subjecting a replica electric grid to cyber-attack.

Despite this, when it comes to resilience, the Government including the NIST Cyber Security Center of Excellence is setting the bar too low. For best results, the value proposition for resilience is based on the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity whether natural or man made under all circumstances of use. Instead, the Government is settling for the operations of withstanding, minimizing, and recovering. Why is this a problem? The most consequential threat to resilience lies in the cascading and propagating triggers that lie hidden in the complexity of critical sector interactions and dependencies inherent in the system of systems that make up the Critical Infrastructure. Without anticipation and avoidance, cascade triggers are left unattended. For example, the Banking and Finance sector must remain ever vigilant during the trading day for evidence of triggers that might impede next day opening of the market. Here anticipation and avoidance including shutdown are preferred over recovery, cleanup, and delayed market opening in maintaining trust in the Banking and Finance sector.

In systems, integration engineering is the process of creating a coherent system from its component parts, both hardware and software, such that at each stage of integration the evolving system exhibits increased functional capability while remaining under firm intellectual control. Integration is a major managerial, technical, and logistical task, requiring the combined efforts of people skilled in systems engineering, hardware engineering, software engineering, and integration engineering. In large systems, software may be the principal integrating element (JSS, 1983).

In systems of systems, integration engineering is the process of combining components and systems and ensuring that the resulting system of systems functions harmoniously. Doing so successfully calls for harmonizing context and culture to eliminate clashes in domain engineering, system architectures, code management, and fielding and sustainability procedures (IBM SJ, 1980). Integration engineering in the pursuit of critical infrastructure resilience is what is needed to harmonize expectations and particular dimensions of diverse industry sectors, to supply intelligent management decision making, to motivate and guide industry sectors on a defined and measured path to resilience maturity, to frame a system of systems architecture capable of supporting digital situation awareness and distributed

supervisory control, and to plan an effective integration program of coordinated activities within a collaborative way of working that will deliver critical infrastructure resilience.

References:

CrossTalk (2011) O'Neill, D., "*Cyber Strategy, Analytics, and Tradeoffs: A Cyber Tactics Study",* CrossTalk, The Journal of Defense Software Engineering, September/October 2011
http://www.crosstalkonline.org/storage/issue-archives/2011/201109/201109-ONeill.pdf

Jacobson, Ivar and Bud Lawson (2015), "*Software Engineering in the Systems Context*", College Publications, Kings College, UK, ISBN-13: 978-1848901766, October 2015, 578 pages

Defense AT&L (2015), O'Neill, D., *"Software 2015: Situation Dire"*, Defense Advanced Technology and Logistics (DAT&L) Magazine, May-June 2015 http://www.dau.mil/publications/DefenseATL/DATLFiles/May-Jun2015/O'Neill.pdf

JSS (1983), O'Neill, D., "*Integration Engineering Perspective*", The Journal of Systems and Software (JSS), 3, 77-83, 1983 http://www.sciencedirect.com/science/article/pii/0164121283900067

IBM SJ (1980) Mills, H.D., O'Neill, D., Linger, R.C., Dyer, M., Quinnan, R.E. (1980) "*The Management of Software Engineering*", IBM Systems Journal (SJ), Volume 19, Number 4, 1980, pages 414-477
http://www.research.ibm.com/journal/sj/

FRAMING RESILIENCE

The Role of the Resilience Integrator

There is a need for a resilience integrator to organize, integrate, and harmonize industry sectors of the critical infrastructure into a resilient system of systems. The stakeholder vision for this project is an opportunity value proposition for operational resilience, one that is capable of anticipating, avoiding, withstanding, minimizing, and recovering from the effects of adversity whether natural or man made under all circumstances of use. The role of Critical Infrastructure Resilience Integration Engineering is being described in five parts:

1. An assessment of the context and culture of industry sectors.
2. An assessment of the readiness to fulfill the Intelligent Middleman job description for each industry sector.
3. An assessment of the Resiliency Maturity Framework for industry sectors.
4. Specification of the Critical Infrastructure Resilience System of Systems Architecture.
5. Preparation of a Program Plan for engineering, developing, integrating, and fielding the Critical Infrastructure Resilience System of Systems in terms of a Way of Working.

If resilience is to be achieved, the resilience integrator must be prepared to provide resiliency engineering features capable of meeting stringent resiliency objectives (Figure 1).

1. The resilience integrator shall harmonize the context and culture of the numerous industry sectors and anticipate domain engineering clashes in order to avoid unintended operations results stemming from diversity in management, process, and engineering approaches.
2. The resilience integrator shall groom Intelligent Middlemen to pave the way in the adoption of the way of working within the industry sectors of the critical infrastructure.
3. The resilience integrator shall facilitate the resilience maturity of management, process, and engineering capabilities and solutions that address security, continuity, survivability, and resilience among the industry sector system of systems.
4. The resilience integrator shall specify a system of systems architecture that facilitates the harmonious cooperation among industry sectors; provide digital situation awareness; allow for distributed supervisor control under stress; and management the assembly, delivery, and control of of common system assets.
5. The resilience integrator shall prepare and coordinate a Resilience Integration Program Plan harmonizing, facilitating, specifying, engineering, developing, integrating, and fielding the critical infrastructure system of systems.
6. The resilience integrator shall frame a way of working to mange the communication, command, control, commitments, and performance among the industry sectors, their contractors, and the resilience integrator including executive councils, steering groups, working groups, and support groups.

Figure 1. Resiliency Objectives and Resiliency Integration Engineering Features

Resiliency Objectives	Resiliency Integration Engineering Features
Anticipating	• Harmonized domain engineering • Coordinated recovery time objectives • Cascade trigger identification • Digital Situation Awareness

Resiliency Objectives	Resiliency Integration Engineering Features
Avoiding	• Shut down • Defense in depth • Operation sensing and monitoring • Distributed Supervisory Control
Withstanding	• Enterprise security • Business process continuity • Survivability • Alternate site
Minimizing	• Adaptation management • Alternate mode • Minimum essential mission • Shut down
Recovering	• Capacity to reorganize • Assured availability • Information and data recovery • Clean up and reconstitution

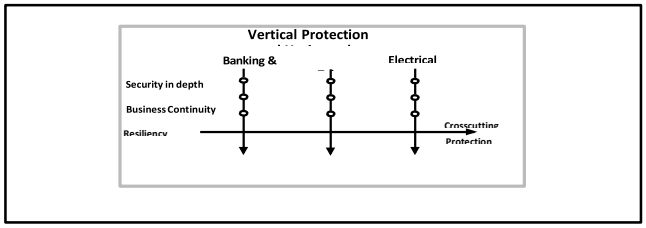
As stated, resiliency is the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity, whether natural or manmade, under all circumstances of use. In order to operational resiliency, objectives must be matched with features.

1. The objective of anticipating calls for the features of harmonized domain engineering, coordinated recovery time objectives, cascade trigger identification, and digital situation awareness.
2. The objective of avoiding calls for the features of shut down, defense in depth, operation sensing and monitoring, and distributed supervisory control.
3. The objective of withstanding calls for the features of enterprise security, business process continuity, survivability, and alternate site.
4. The objective of minimizing calls for the features of adaptation management, alternate mode, minimum essential mission, and shut down.
5. The objective of recovering calls for the features of capability to reorganize, assured availability, information and data recovery, and clean up and reconstitution.

Dimensions of Resiliency

Resiliency is the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity, whether natural or manmade, under all circumstances of use. Resiliency applied to a system of systems focuses on crosscutting issues. Crosscutting effects stem from dependent relationships (Figure 2). Some dependent relationships are planned and intended interactions between industry sectors, such as, financial transactions embedded in telecommunications, electrical, transportation, and medical operations. Other dependent relationships are indirect and stem from outsourced commoditized services that bring with it opportunities for common single point failures among industry sectors, such as, the Internet, the Global Positioning System, Federal Express, and common vendors.

Figure 2. Vertical Protection and Horizontal Resilience



One respected researcher seemed to concede the high ground of resiliency, that is, avoidance, in associating resilience with the Timex slogan, *"Take a licking and keep on ticking".* The question then becomes what perimeter is being secured? In protecting a network node or a physical facility in a geographic region, each node or facility is to be protected and made survivable. In achieving resilience, propagation and cascading effects across the network and region must also be curtailed. This is made difficult by context and culture challenges of the industry sectors within the critical infrastructure.

The capabilities needed to impact crosscutting issues cannot be expected to evolve in a loosely coupled environment. They must be holistically specified, architected, designed, implemented, and tested if they are to operate with resilience under stress. A management, process, and engineering maturity framework is necessary to advance the assurance of software security, business continuity, system survivability, and system of systems resiliency capabilities.

Resiliency Assurance

What is software assurance? According to the Department of Homeland Security (DHS) software assurance (CrossTalk, 2014.1) spans:

1. Trustworthiness - No exploitable vulnerabilities exist, either maliciously or unintentionally inserted.
2. Predictable Execution - Justifiable confidence that software, when executed, functions as intended
3. Conformance - Planned and systematic set of multi-disciplinary activities that ensure software processes and products conform to requirements, standards, and procedures.

How are these attributes achieved? All of this flows from a well stated value proposition and the requirements and user stories that depend on achieving intended outcomes beginning with the harmonization of critical infrastructure industry sector context and culture. Ultimately the intended outcome of resiliency is the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity whether natural or manmade under all circumstances of use.

What about risk? Risk is uncertainty and the prospect for loss or gain depending on the outcome of an event. An industrial strength software risk management practice is one that treats risk as uncertainty and carefully distinguishes risks from the sources of risk and problems. Since risk is uncertainty, the challenge is to calculate the uncertainty of a risk and accept only those risks whose joint probability of occurrence and prospect for loss or gain are prudent choices. These are considered calculated risks.

Are there uncertainties? The uncertainties in the achievement of critical infrastructure resiliency assurance are many. Beginning with readiness, uncertainties span will, commitment, capabilities, deployment, and execution. Associated with these, there needs to be affirmative assertions coupled with compelling arguments backed up with convincing evidence. Appendix A lists the convincing evidence associated with the integrating elements of critical infrastructure resiliency assurance, all based on the story that will unfold in this article. Where affirmative assertions are false whether through ignorance, oversight, neglect, or intent, an organization is at risk of a false claims charge. Careful, complete, and correct assurance steps coupled with diligent risk management provide the best safeguard against false claims.

Reference:

CrossTalk (2014.1) O'Neill, D., *"Software Assurance, Trustworthiness, and Rigor*", CrossTalk, The Journal

of Defense Software Engineering, September/October 2014
http://www.crosstalkonline.org/storage/issue-archives/ 2014/201409/201409-ONeill.pdf

FRAMING CRITICAL INFRASTRUCTURE

Critical Infrastructure Sectors

The critical infrastructure is composed of the numerous industry sectors that do the heavy lifting. Some key sectors are listed here.

1. Utilities and Energy contain power generation and distribution systems, nuclear power control systems, and energy resource allocation systems.
2. Telecommunications contain network control and switching systems, satellite control and management systems, and mobile communications systems and protocols.
3. Banking and Finance contains electronic commerce and electronic funds transfer systems, transaction processing systems, security and privacy management systems, and network management systems.
4. Transportation contains route management and collision avoidance systems, avionics systems, air traffic control systems, navigation and position location systems, and embedded automobile control systems.
5. Medical Systems contain medical device control systems, patient record systems, and insurance and payment systems.

Cascade Triggers

Each critical infrastructure industry sector is dependent on other industry sectors. The interdependence of electric power, telecommunications, energy, financial, transportation, emergency services, water, food, and so forth is exacerbated by the embedded electronic devices relied on to provide critical controls. Electric power and telecommunications stand out as common critical dependencies for all industry sectors and require special preparation and protection measures. Underneath the surface and hidden in the complexity of critical sector interactions and dependencies are triggers that can result in cascading and propagating effects and impacts.

Mostly hidden, cascade triggers may stem from known conditions and system states including the flash crash, electrical grid physical infrastructure vulnerability, Internet Distributed Denial of Service (DDOS), cyber crime, and encryption based on deterministic mathematical certainty.

The Flash Crash took advantage of data transmission and trading speed differentials that resulted in wide swings in markets prices. Buyers in the futures markets included high-frequency trading firms that buy and sell within minutes. Their tactics of spoofing, layering and front-running are now banned.

Hidden or in plain sight, cascade triggers are capable of invading various industry sectors in a variety of ways. The transportation sector can be brought to its knees if truck drivers cannot use credit cards to charge for gas tank fill ups. The medical sector depends on the Internet to distribute and present patient electronic medical records on demand. The electrical grid depends on a survivable electrical grid with predictable demand profiles matched to planned resources and capacities. The banking and finance sector remains ever conscious of its need to protect next day opening even in the presence of a flash crash disruption. The users of the telecommunications sector are increasingly vulnerable to Internet disruptions like DDOS, and encryption-based scams like ransomware.

Anticipating, avoiding, and minimizing the effects of these triggers is a responsibility of the resiliency integrator. For example, the Banking and Finance sector must remain ever vigilant during the trading day for evidence of triggers that might impede next day opening of the market. Here anticipation and avoidance is preferred over recovery, cleanup, and delayed market opening in maintaining trust in the Banking and Finance sector.

Banking and Finance Sector Cascade Trigger Use Case

The Banking and Finance sector illustrates the stovepipe cultural environment and technological vulnerabilities that stand ready to trigger societal impact. Its institutional dependence on public trust and its operational dependence on electrical and telecom resilience under stress with its tightly coordinated recovery time objectives make it vulnerable (Jacobson, 2015).

In banking and finance, the financial services industry depends on a network of systems that process instruments of monetary value in the form of deposits, loans, funds transfer, savings, and other financial transactions. The network is composed of banks, other depository institutions, and the Federal Reserve System as well as underwriters, brokerages, and mutual funds. In addition there are industry utilities including the New York Stock Exchange (NYSE), the Automated Clearing House (ACH), Depository Trust Clearinghouse Corporation (DTCC), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT) as well as underlying third party electronic processing services (EMP, 2004).

The Interagency Paper (Bank, 2001) pinpoints clearing and settlement systems as the most critical business operations at risk for financial markets and the disruptions of clearing and settlement processes would have an immediate systemic effect on critical financial markets. The use of the term "systemic risk" is based on the international definition of systemic risk in payments and settlement systems (FED et al, 2002).

The Federal Reserve Board specified that the following functions are critical to the operation and liquidity of banks and stability of financial markets and require same day recovery:

1. Large–value inter-bank funds transfer, securities transfer, or payment-related services, such as Fedwire, Clearing House Interbank Payments System (CHIPS), Depository Trust Clearinghouse Corporation (DTCC), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT)
2. Automated clearinghouse (ACH) operators
3. Key clearing and settlement utilities
4. Treasury automated auction and processing system
5. Large-dollar participants of these systems and utilities

The banking sector depends on maintaining the trust of the banking community and the banking public. In large measure this trust is maintained through the transparency and verification inherent in exchanges. Without this trust the banking system itself risks anarchy. Overall, the stock exchanges and their associated clearinghouses have performed due diligence and taken the steps necessary to ensure the resilience of their operations.

1. Under what circumstances might the trust in the banking system be tested and stressed? At the close of each business day it is the expectation and practice of the banking community that the banking ledgers of branch offices be reconciled and balanced to the penny and that securities and trading firms create a daily P&L.

2. Under what circumstances of use might the banking ledgers be thrown out of balance impacting the daily closing and settlement process… and the next day opening?
3. More specifically what is the least Cyber Security exploit capable of impacting next day closing?

References:

Bank (2001) *A Glossary of Terms in Payment and Settlement Systems*, Committee on Payment and Settlement Systems, Bank for International Settlements, 2001.

EMP (2004) *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, Volume 1: Executive Report, 2004.

FED et al (2002) *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System,* The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, September 5, 2002.

Jacobson, Ivar and Bud Lawson (2015), *"Software Engineering in the Systems Context",* College Publications, Kings College, UK, ISBN-13: 978-1848901766, October 2015, 578 pages.

Critical Infrastructure Challenges

The critical infrastructure is composed of the numerous industry sectors that do the heavy lifting. Some key sectors include Utilities and Energy, Telecommunications, Banking and Finance, Transportation, and Medical Systems. The operations within the industry sectors of the critical infrastructure are diverse and complex. These industry sectors comprise an accidental system of systems that intersect operationally without a plan and design in advance. Each sector system was constructed within its own context and culture. In operation, these sector systems may inadvertently impose their own context and culture on others and clash with uncertain and unintended operational results.

1. Industry sector practice varies widely in their domain engineering approaches resulting in diversity in architecture, models, and patterns including their representation. Formality within an architectural framework facilitates the imposition of distributed supervisory control, interoperability, and operation sensing and monitoring protocols.
2. Industry sector maturity in management and engineering processes varies widely resulting in diversity in configuration management, frequency of release, conformance to requirements, and traceability among life cycle artifacts. Strong code management practices facilitate reconfiguration and reconstitution.
3. Industry sector practice varies widely in fielding and operating practices resulting in diversity in accountability and control, supply chain management, civility and pushback, and willingness to expend off the clock effort. Exercising strong control over the workforce facilitates business continuity and survivability.
4. Industry sector impacts from government regulation vary with respect to export control, tax policy, intellectual property, privacy, and antitrust litigation. Exercising strong government control facilitates compliance for the benefit of the commons at the expense of initiative for the self-interest.
5. Industry sector public expectation and confidence vary with respect to trust, loyalty, and satisfaction. The financial and medical sectors depend on public trust. The electrical and telecommunication sectors depend on customer loyalty and satisfaction. The diverse industry sector expectations of trust, loyalty, and satisfaction must be respected, blended, and harmonized.

6. Technical debt is the organizational, project, or engineering neglect of known good practice that can result in persistent public, user, customer, staff, reputation, or financial cost. In truth most technical debt is taken on without this strategic intent, without even knowing it, and without the wherewithal in capability or capacity to do the job right. Technical debt must be eliminated.
7. Underlying cascading and propagating triggers hidden in the complexity of critical sector interactions and dependencies must be anticipated, avoided, and minimized.
8. Industry sector software sourcing diversity introduces a range of business, legal, technical and management exposures that must be dealt with in the best possible way.
9. Supply chain risk management assurance involves the assessment of trust in the chain of custody of components, the detection of counterfeit and tainted components, and much more.
10. Cyber security strategy and tactics involves anticipation, protection, detection, attribution, and counter measures.

Consequently, the following context and culture harmonization guidance is offered:

1. Formality within an architectural framework facilitates the imposition of distributed supervisory control, interoperability, and operation sensing and monitoring protocols.
2. Strong code management practices facilitate reconfiguration and reconstitution.
3. Exercising strong control over the workforce facilitates business continuity and survivability.
4. Exercising strong government control facilitates compliance for the benefit of the commons at the expense of initiative for the self-interest.
5. The diverse industry sector expectations of trust, loyalty, and satisfaction must be respected, blended, and harmonized.
6. Technical debt must be eliminated.
7. Cascading and propagating triggers must be anticipated, avoided, and minimized.
8. Industry sector software sourcing exposures must be understood and managed.
9. Supply Chain Risk Management operations must be assured.
10. Cyber security strategy policy decisions and defined tactics must be assured.

RESILIENCE INTEGRATION ISSUES

Formality Within an Architectural Framework

Industry sector practices vary widely in their domain engineering approaches resulting in diversity in architecture, models, and patterns including their representation. Formality within an architectural framework facilitates the required imposition of distributed supervisory control, interoperability, and operation sensing and monitoring protocols. Crosscutting industry sector dependencies elevate the imperative for the sacrifices needed. It is here that the resilience integrator and the Intelligent Middlemen discussed later have their work cut out for them.

Resiliency domain engineering procedures associated with adaptation management, capacity to reorganize, distributed supervisory control, digital situation awareness, and coordinated recovery time objectives are not trivial application appendages or extensions. Instead their implementation involves designing and invoking interfaces to operating system services accessible either directly or through middleware. For best results, domain engineering for resilience should employ common models and patterns for each industry sector.

Strong Code Management Practices

Industry sector maturity in management and engineering processes varies widely resulting in diversity in

configuration management, frequency of release, conformance to requirements, and traceability among life cycle artifacts. Strong code management practices facilitate reconfiguration and reconstitution (IBM SJ, 1980).

Code management practices are highly situational and depend on the particular vendor history and evolution of legacy practices and tools; the knowledge and skills of the technical staff on hand; modernization strategies in effect and management in place; and particular engineering, developing, integrating, and fielding needs of an industry sector dictated by its cultural drivers of trust, loyalty, and satisfaction.

For best results, commonality in code management practices should be sought across industry sectors without disadvantaging any industry sector. Particular attention must be paid to arriving at a coordinated software patching policy, one that maintains interoperability dependencies and sustains the necessary frequency of release dynamics and expectations among industry sectors.

Reference:

IBM SJ (1980) Mills, H.D., O'Neill, D., Linger, R.C., Dyer, M., Quinnan, R.E. (1980) "*The Management of Software Engineering*", IBM Systems Journal (SJ), Volume 19, Number 4, 1980, pages 414-477 http://www.research.ibm.com/journal/sj/

Strong Industry Sector Control Over the Workforce

Supplier control is achieved within an industry sector by establishing an attractive workplace culture, achieving maturity in process and skills, deepening industry relationships, and retaining personnel (CrossTalk, 2003).

- More than any other profession, the programming workplace culture must match the nature of the workers and the work they do. It revolves around true civility among peers and genuine appreciation by management for the essential contribution programmers are making to the enterprise and the nation. Programming employs a process of experimentation where the hypotheses are function, form, and fit. Much of the programmers' work is both creative and conforming at the same time as they seek the best mix of requirements, data structures and constructs, and execution paths. In establishing an attractive workplace culture, the leading indicators of behaviors to understand well include civility, push back, commodity view, and management ignorance. The leading indicators of rewards to manage well include competitive wage structures, key employee status, and investment contribution. The leading indicators of outcomes to measure and guide include personnel overtime, off the clock time, employee morale, and team satisfaction.
- Providing the right skills, at the right time, and in the right place is a difficult combination to achieve in an environment of rapid change and personnel shortages. The leading indicators for achieving maturity include software skills and personnel certification. The leading indicators of outcome include software productivity and span of responsibility. With skilled personnel and organization software process maturity, the leading indicators to manage well include accountability and control, commitment management, predictable performance, and modern software engineering practices.
- A variety of industry relationships are needed to control resources. Sources for outsourcing both domestic and offshore are highly valued. The agenda for supplier bargaining power, immigration policy, and unionization demands active participation by the enterprise. The outcome is measured in terms of open requisitions, personnel turnover, and staff churn and their impact on products and services.
- Software personnel are in great demand to support industries of all kinds. Retaining software

personnel who have learned the application domain and the trade secrets of an enterprise is essential. The leading indicators for retaining software personnel include competitive wage structures and key employee status. The leading indicators of outcome to measure include open requisitions, personnel turnover, and staff churn.

Industry sector practice varies widely in fielding and operating practices resulting in diversity in accountability and control, supply chain management, civility and pushback, and willingness to expend off the clock effort. Exercising strong control over the workforce facilitates business continuity and survivability.

Human resource practices vary from industry sector to industry sector. These practices involve variable tolerance for off the clock time and overtime, irregular shift schedules, daily local travel, long distance overnight travel demands considered acceptable. In delivering resilience under stress, common protocols might involve shutdown, alternate mode, or alternate site. In addition, it might be necessary to adjust to the stresses of an incident immediately and completely. For example, consider a Manhattan operation having to immediately populate an alternate site in eastern Pennsylvania for days or even weeks.

Reference:

CrossTalk (2003) O'Neill, D., "*Introducing Global Software Competitiveness"*, CrossTalk, The Journal of Defense Software Engineering, Online Articles, October 2003
http://www.crosstalkonline.org/storage/issue-archives/ 2003/200310/200310-ONeill.pdf

Strong Government Control Over Industry Sectors

Industry sector impacts from government regulation vary with respect to export control, tax policy, intellectual property, privacy, and antitrust litigation. Exercising strong government control facilitates compliance for the benefit of the commons at the expense of initiative for the self-interest.

Accommodating the national interest and taking direction from government personnel during a crisis may be a possibility for which participants should be prepared to tolerate and endure without pushback as a condition of employment. For example, the more controversial attitudes and practices associated with privacy and sharing intellectual property should be sorted out beforehand and should not become distractions during an active incident.

Expectations of Trust, Loyalty, and Satisfaction

Industry sector public expectation and confidence vary with respect to trust, loyalty, and satisfaction. The financial and medical sectors depend on public trust. The electrical and telecommunication sectors depend on customer loyalty and satisfaction. The diverse industry sector expectations of trust, loyalty, and satisfaction must be respected, blended, and harmonized. The diverse industry sector expectations of trust, loyalty, and satisfaction must be respected, blended, and harmonized.

While it may be possible to respect these deeply ingrained cultural expectations, blending and harmonizing these expectations may lie outside the realm of possibility (CrossTalk, 2012).

1. An organization driven by reputation and avoiding the risk of loss of trust may place a high value on trustworthiness and security along with the steps needed to assure these attributes. The telecommunications, financial services, and medical sectors where trust is all-important fit the reputation scenario.
2. An organization driven by economics may place a high value on profitability and attributes like cost control, productivity, and span of responsibility. The financial services, manufacturing, and utilities and energy sectors fit the economics scenario.
3. An organization driven by mission may place a high value on sustainability, capability control, and capacity control as well as reliability, availability, security, and resiliency. The telecommunications, transportation, medical, and defense sectors fit the mission scenario.
4. An organization driven by competitiveness may place a high value on release frequency, time to market, and innovation as well as cost and schedule control and predictability control (CrossTalk 2003). The manufacturing and e-commerce sectors fit the competitiveness scenario.
5. An organization driven by outsourcing may place a high value on release frequency, time to market, and innovation as well as quality control, configuration management, and span of responsibility of onshore staff. The manufacturing sector fits the outsourcing scenario.
6. An organization driven by high assurance may place a high value on trustworthiness including quality control, defect free, predictability control, resiliency, and frequency of release. The telecommunications, financial services, transportation, medical, and defense sectors fit the high assurance scenario.

References:

CrossTalk (2012) O'Neill, D., *Extending the Value of the CMMI to a New Normal",* CrossTalk, The Journal of Defense Software Engineering, January/February 2012
http://www.crosstalkonline.org/storage/issue-archives/2012/201201/201201-ONeill.pdf

CrossTalk (2003), "Introducing Global Software Competitiveness", CrossTalk, The Journal of Defense Software Engineering, Online Articles, October 2003
http://www.crosstalkonline.org/storage/issue-archives/ 2003/200310/200310-ONeill.pdf

Technical Debt Elimination

Technical Debt is the organizational, project, or engineering neglect of known good practice that can result in persistent public, user, customer, staff, reputation, or financial cost (Defense AT&L, 2013). In truth most Technical Debt is taken on without this strategic intent, without even knowing it, and without the wherewithal in capability or capacity to do the job right. Technical Debt must be eliminated.

In order to achieve the attributes of trustworthiness, predictable execution, and conformance, the software operations in each industry sector of the critical infrastructure must be free of Technical Debt. Shortcuts, expedient activities, and poor practice contributing to the initial product launch or initial operational capability are often cited as justifiable excuses in taking on Technical Debt; but in truth most Technical Debt is taken on without this strategic intent, without even knowing it, and without the

wherewithal in capability or capacity to do the job right. In any event, as the twig is bent so grows the tree, and the weight of accumulated Technical Debt immediately and continuously extracts its cost on the organization.

1. Technical Debt is considered written off only when it is eliminated. Draining the swamp depends on understanding and aligning the sources of Technical Debt in management, engineering, and process.
2. Sources of Technical Debt in engineering involve neglect in application domain understanding, requirements determination, system and software architecture, iterative multi-level design, staged incremental development, software development life cycle, programming language, middleware, operating system, network interface, and software development environment.
3. Sources of Technical Debt in management involve neglect in requirements management, estimating, planning, measurement, monitoring and controlling, risk management, process management, team innovation management, supply chain management, team building, personnel management, and customer relationship management.
4. Sources of Technical Debt in process involve insufficient evidence of explicit goals and readiness to perform, insufficient accountability based on work responsibility matrix, insufficient planning of design levels and staged increments, and insufficient planning, management, and control of software product releases.

Reference

Defense AT&L (2013) O'Neill, D., *"Technical Debt in the Code: Cost to Software Planning",* Defense Advanced Technology and Logistics (DAT&L) Magazine, March-April 2013
http://www.dau.mil/pubscats/ATL%20Docs/Mar_Apr_2013/O%27Neill.pdf

Cascade Trigger Anticipation

Underlying cascading and propagating triggers hidden in the complexity of critical sector interactions and dependencies must be anticipated, avoided, and minimized. Each critical infrastructure industry sector is dependent on other industry sectors. The interdependence of electric power, telecommunications, energy, financial, transportation, emergency services, water, food, and so forth is exacerbated by the embedded electronic devices relied on to provide critical controls. Electric power and telecommunications stand out as common critical dependencies for all industry sectors and require special preparation and protection measures.

Underneath the surface and hidden in the complexity of critical sector interactions and dependencies are triggers that can result in cascading and propagating effects and impacts. Anticipating, avoiding, and minimizing the effects of these triggers is a responsibility of the resiliency integrator. For example, the Banking and Finance sector must remain ever vigilant during the trading day for evidence of triggers that might impede next day opening of the market. Here anticipation and avoidance is preferred over recovery, cleanup, and delayed market opening in maintaining trust in the Banking and Finance sector.

Software Product Sourcing Exposures

The provenance and pedigree of source code matters. Industry sector software sourcing diversity introduces a range of business, legal, technical and management exposures that must be dealt with in the best possible way. Industry sector software sourcing exposures must be understood and managed.

The various industry sectors of the critical infrastructure exhibit diversity in the manner in which their

software products are sourced including in-house development, open source, contract acquisition, and outsourcing both domestic and global offshore (CyLab, 2008). Whatever the means, industry sectors subject to integration engineering in the pursuit of resiliency and the data and information this entails face a range of exposures including business and legal, cultural, technical and legal, and software engineering and management.

1. In the business and legal domain, the management and control of intellectual property requires that the boundary between legal and technical factors be spanned with confidence including additional privacy, increased anonymity, adequate safeguard of proprietary assets, and due diligence against bold assertions that invite false claims charges.
2. In the cultural domain, misunderstandings and expectation shortfall must be dampened without damaging relationships, but at the same time issues must be handled in the best possible way not simply accommodated.
3. In the technical and legal domain, piracy of software packages must be controlled, and the workforce must be vetted. In addition the interoperability of multi-sourced software products must be assured in all circumstances or use.
4. In the software engineering and management domain, a balance must be sought among software process maturity, software product engineering, and the process of experimentation essential to innovation, one that facilitates a rapid, predictable, and reliable operation operation and is accorded the best possible management, oversight, and governance along with a seat in the boardroom.

References:

CyLab (2008), O'Neill, D., "*Inside Track to Offshore Outsourcing Using the Trusted Pipe™: What Global Enterprises Look For in Offshore Outsourcing",* Making the Business Case for Software Assurance Workshop, Carnegie Mellon CyLab, Pittsburgh, PA, September, 2008, pages 59-75

Supply Chain Risk Management Assurance

The Department of Defense, the defense industrial base, and the nation's critical infrastructure all face challenges in Supply Chain Risk Management Assurance. These diverse challenges span infrastructure, trust, competitiveness, and austerity. Beginning with acquisition where Supply Chain foundations are laid, Supply Chain Risk Management Assurance extends into operations and sustainment (CrossTalk, 2014.2).

While Supply Chains are essential to global competitiveness and national security, Supply Chains in the wild are intrinsically risky, vulnerable to Cybercrime and Cloud Computing risks as well as organizational neglect and unmet needs. The practice of risk management using smart and trusted tactics is necessary because software-based supply chains are inherently insecure, the risks and uncertainties are prolific, and vulnerabilities abound. The combination of unmet needs, industry neglect, and austerity coupled with the immature state of software, Cyber Security, and Cloud Computing infrastructure yield a rich environment of uncertainty and risk in establishing and maintaining infrastructure, being trusted, being competitive, and being austere.

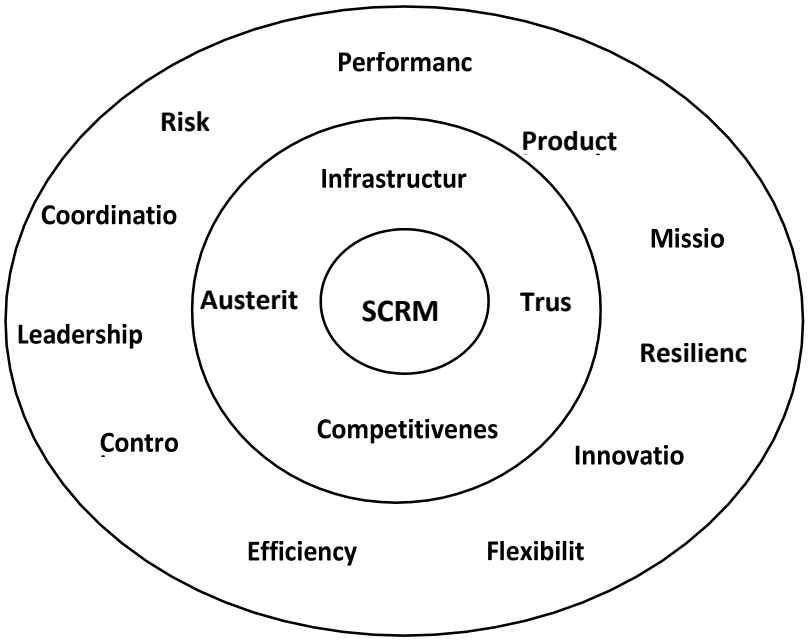
Each industry sector has an associated supply chain essential to the engineering, developing, integrating, and fielding of industry sector capabilities and systems. Supply Chain Risk Management (SCRM) Assurance involves the assessment of trust in the chain of custody of components, the detection of counterfeit and tainted components, and much more.

The role of resilience integrator is to encourage, stimulate, and incentivize supply chain owners and operators to positively and proactively assure the identification, mitigation, transfer, or acceptance of the sources of risk, problems, and factors that may impede the achievement of supply chain goals and objectives. Supply Chain Risk Management Assurance operates under three levels of indirection. First, it is a *framework*, a basic underlying structure. Second, it promises *assurance*, a positive declaration intended to inspire confidence. Third, it *manages risk* through the identification, elimination, mitigation, transfer, or acceptance of factors, sources of risk, and problems that may impede the achievement of supply chain goals and objectives.

1. As a framework, Supply Chain Risk Management Assurance focuses on the infrastructure of management, engineering, process, technology, and skills needed to acquire, field, and operate trusted, competitive, and austere software-based supply chains with intelligence and confidence.
2. As an assurance mechanism, Supply Chain Risk Management Assurance validates positive declarations intended to inspire confidence using assurance assertions and levels of confidence.
3. As a risk mechanism, Supply Chain Risk Management Assurance seeks to prudently assign the disposition of risks associated with factors, sources of risk, and problems and to calculate the risk associated with supply chain goals and objectives.

Setting goals is the first step in managing risk. Goals are attributes to be assured. Goals associated with smart and trusted Software and Supply Chain Risk Management Assurance include maintaining infrastructure, being trusted, being competitive, and being austere. Objectives associated with goals are factors with consequential outcomes, for example, performance, product integrity, mission, resilience, innovation, flexibility, efficiency, control, leadership, coordination, and risk (Figure 3).

Figure 3. Supply Chain Risk Management Assurance: Strategic Goals and Tactical Objectives



References:

CrossTalk (2014.2) O'Neill, D.,*"Software and Supply Chain Risk Management Assurance Framework",* CrossTalk,
The Journal of Defense Software Engineering, March/April 2014
http://www.crosstalkonline.org/storage/issue-archives/2014/201403/201403-ONeill.pdf

Cyber Security Strategy and Tactics

A strategy is an overarching plan to achieve a vision along with the policies and protocols that link and coordinate the tactics employed. In Cyber Security time matters and things move fast, at the speed of light... faster than people can close their command and control loops. So a Cyber Strategy must include the policy to authorize in advance time critical actions based on tradeoffs that have carefully weighed cause, effect, and consequences. It is through continuously rebalanced tradeoffs and adjustments in the policy authorizing time critical actions that a strategy retains its currency in the face of new knowledge and new threats (CrossTalk, 2011).

A Cyber Strategy is a policy composed of a collection of defined tradeoffs made in advance with implementing tactics ready for deployment. For example:

1. Where the inevitability of a Cyber Attack is a given, the power of trading off acceptance of some consequences in order to avoid or limit other consequences should not be ignored. How much lost opportunity, loss of availability, and loss of privacy are we willing to trade off to avoid cleanup and recovery costs and loss of trust impact?
2. The power of the shutdown as a tactical instrument to trade off consequences should not be underestimated. Upon shutdown, we immediately incur lost opportunity and loss of availability in order to avoid or limit cleanup and recovery costs and loss of trust and loss of privacy impacts.
3. The power of the social contract as an instrument to implement trade offs should not be overlooked. Where civility is defined as the sacrifices we make for others, perhaps an appeal to civility would prompt people to agree to sacrifice some level of privacy in order to promote a higher level of security for others. Here civility would lubricate the trade off between security and privacy. However, the catalyst needed to spark the social contract is leadership, not always available.

Trading off consequences is situational. For example, consider the priority ranking of consequences by reputation, economics, mission, and competitiveness. There are consequences in prioritizing consequences.

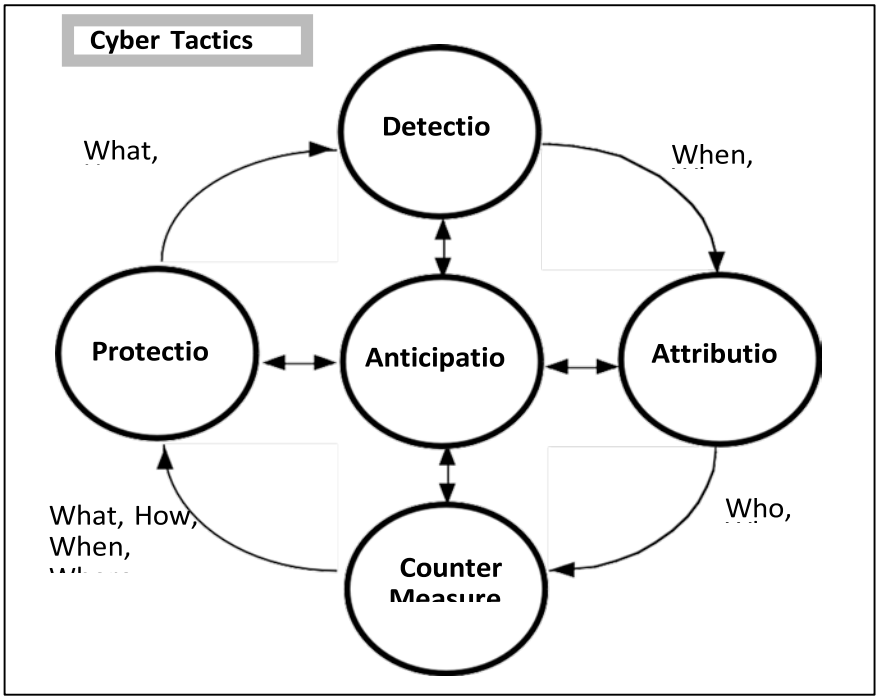
1. In the reputation scenario, the highest consequences to avoid are loss of trust and loss of privacy followed by lost opportunity and loss of availability and then cleanup and recovery. The financial services sector where trust is all-important fits the reputation scenario.
2. In the economics scenario, an organization may place a high value on profitability where the highest consequences to avoid are lost opportunity and loss of availability followed by cleanup and recovery and then loss of trust and loss of privacy. The energy sector fits the economics scenario.
3. In the mission scenario, an organization may place a high value on ensuring continuous operation where the highest consequences to avoid are lost opportunity, loss of availability, and loss of trust followed by loss of privacy and then cleanup and recovery. The telecommunications

sector fits the mission scenario.

4. In the competitiveness scenario, an organization may place a high value on its proprietary information where the highest consequences to avoid are lost opportunity, loss of trust, and loss of privacy followed by cleanup, recovery, and perhaps loss of availability. The e-commerce sector fits the competitiveness scenario.

Cyber Tactics (Figure 4) span anticipation, protection, detection, attribution, and counter measures (Table 2). However, these Cyber Tactics are currently underdeveloped and insufficient as implementers of the nation's Cyber Strategy. Until these Cyber Tactics evolve to a more robust level of professional maturity, the nation's Cyber Strategy will continue to be framed in the political domain with its unresolved clashes of philosophy. Without a framework of Cyber Tactics, the nation's Cyber Strategy will continue to remain unhinged.

Figure 4. Trusted Pipe™ Cyber Tactics Framework



® Trusted Pipe is registered with the U.S. Patent and Trademark Office by Don O'Neill

ANTICIPATION

1. The intended function of anticipation is to make decisions about the future based on expectation in order to anticipate, avoid, withstand, minimize, and recover from the effects of adversity under all circumstances. Unlike other tactics, anticipation takes place before an attack.
2. Cause and effect forward chain traces are used in order to interdict cause primarily in terms of Cyber
Security goal selection, standard of excellence attributes for software engineered products, and

economic cost impact and end user mission loss consequences. A secondary cause and effect thread composed of common weaknesses, attack outcomes, and bad actors may also inform anticipation tactics and serve to verify the primary thread.

3. The pursuit of anticipation tactics contributes to an understanding of *what and how* in terms of weaknesses and vulnerabilities, build security in maturity, and security in depth.

PROTECTION

1. The intended function of protection is to deploy effective safeguards to impede attack outcomes including unauthorized access, loss of data, tampering with data, erosion of performance, and denial of service.
2. Protection is informed by known weaknesses and vulnerabilities and their connection to attack outcomes.
3. Protection tactics reflect an understanding of *what* and *how* in deploying defense in depth mechanisms including encryption, identity management, access control, authorization management, accountability management, configuration management, and security assurance operations.

DETECTION

1. The intended function of detection spans digital situation awareness, operation sensing and monitoring, and the identification of defects, weaknesses, vulnerabilities, attacks, outcomes, and bad actors through monitoring, inspection, assessment, deep analytics, surveillance, alertness, and awareness.
2. The collection of dynamic operations sensing and monitoring logs fuels an activity of deep analytics. The systematic inspection of life cycle systems and software artifacts by experts reveals defects, weaknesses, and vulnerabilities from which attacks are composed. The automatic static analysis of software code, both source and object, also fuels an activity of deep analytics. As common weaknesses, common vulnerabilities, and common attack profiles emerge, they become patterns and templates for subsequent surveillance.
3. Detection tactics contribute to an understanding of *when* and *where* in terms of defects, attacks, outcomes.

ATTRIBUTION

1. The intended function of attribution is focused on the assessment of cause and effect trace artifacts to identify a person, account, group, or intermediary responsible or involved.
2. Cause and effect backward chain traces are used in order to profile the cause in terms of attack outcomes, bad actors, and economic cost impact and end user mission loss consequences.
3. Attribution tactics contribute to an understanding of *who* and *why* in terms of motivation and rationale, exploits employed, intended attack outcomes, and consequences sought.

COUNTER MEASURES

1. The intended function of counter measures is focused on the detection and elimination of common weaknesses; adherence to rigorous standard of excellence attributes of completeness, correctness, and rules of construction; elimination of attack outcomes; strengthening defenses against bad actors; and avoiding, withstanding, mitigating, and recovering from consequences.
2. Actual *when* and *where* in terms of defects, attacks, outcomes and actual *who* and *why* in terms of motivation, intended attack outcomes, and consequences sought provide the fuel for

composing effective counter measures.

3. Counter measures tactics are focused on understanding *what and how, when and where, and who and why*
   in terms of counter measures to interdict weaknesses and vulnerabilities, to build security in, and install security in depth.

References:

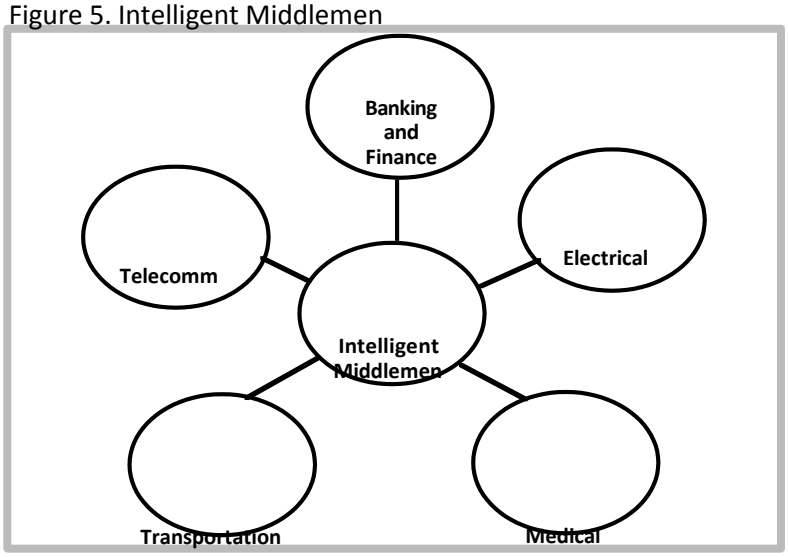
CrossTalk (2011) O'Neill, D., "*Cyber Strategy, Analytics, and Tradeoffs: A Cyber Tactics Study",* CrossTalk, The Journal of Defense Software Engineering, September/October 2011
http://www.crosstalkonline.org/storage/issue-archives/2011/201109/201109-ONeill.pdf

INTEGRATING ELEMENTS OF RESILIENCE

Intelligent Middlemen

Intelligent Middlemen possess the broad range of hard and soft skills spanning the cultural, ethical, legal, business, process, management, and engineering dimensions needed to meet the challenges of the critical infrastructure in anticipating, avoiding, minimizing, withstanding, and recovering from crosscutting effects and to impede the emergence of propagating and cascading effects. The Intelligent Middlemen are positioned at the center of things and serve as the traffic cop for identifying and driving resolution of crosscutting issues (Figure 5).

Figure 5. Intelligent Middlemen



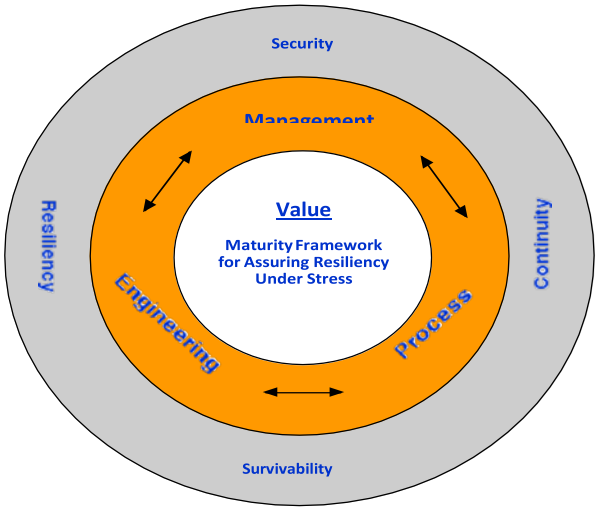
The Intelligent Middleman job description is specified as follows:

1. The Intelligent Middleman must be educated, trained, and in possession of the broad gauge experience to fill the role of Chief Critical Infrastructure Resilience Architecture and Operations Engineer.
2. As Chief Engineer, the Intelligent Middleman must be educated and trained in the prerequisite essentials of both systems engineering and software engineering and have experience in how things are built and how things are used from architecture through operations.
3. As a boundary spanner, the Intelligent Middleman must understand and be capable of planning and exercising command and control of the critical infrastructure under stress.
4. Specifically, the Chief Engineer must mange the state transitions associated with its electrical grid and data transmission infrastructure, interoperability and information sharing protocols, Cyber Security framework, law enforcement and emergency services, sector coordinated recovery time objectives, cascade triggers digital situation awareness, information and data recover protocols, distributed supervisory command and control protocols, and supply chain logistics and risk management.
5. The Intelligent Middleman must maintain the foremost focus on the goal of anticipating, avoiding, withstanding, mitigating, and recovering from the effects of adversity whether natural or manmade under all circumstances of use.

Maturity Framework for Assuring Resiliency Under Stress

There exists a need for a means to harmonize the diverse and complex operations within the industry sectors of the critical infrastructure which comprise an accidental system of systems that intersect operationally without a plan and design in advance. The Maturity Framework for Assuring Resiliency Under Stress (CrossTalk, 2009) provides that means and delivers value through management, process and engineering capabilities and solutions that address security, continuity, survivability, and resiliency (Figure 6).

Figure 6. Maturity Framework for Assuring Resiliency Under Stress



The system perimeter focus areas include commitment to a business case, security in depth, business continuity, and survivability. The essential focus areas needed to extend this perimeter to the system of systems context needed to demonstrate resiliency include coordinated recovery time objectives,

interoperable information and data exchange, operation sensing and monitoring, distributed supervisory control, and information and data recovery. To achieve maturity in the assurance of resiliency under stress, the enterprise must satisfy the goal-based argument at each level. The objective of the Maturity Framework for Assuring Resiliency is to drive the business case and enterprise commitment towards the assurance of software security, business continuity, system survivability, and system of systems resiliency.

Level 1 Ad Hoc

- State of Affairs: Inability to advance and exhibiting evidence of apathy, denial, management inaction, and lack of engineering know how.
- Issue Areas: Apathy, State of Denial, Management Inaction, Lack of Engineering Know How.

Level 2 Enterprise Security Commitment Management

- Goal: Demonstrate commitment to security assurance through strategic management, internal processes, and defense in depth.
- Focus Areas: Global Software Competitiveness, Competitiveness Versus Security, CSO Leadership Program, Security Return on Investment, Security Assurance Operations.

Level 3 Enterprise Business Continuity Process Maturity

- Goal: Demonstrate business continuity assurance through compliance management, external processes, and product engineering.
- Focus Areas: Global Sourcing, Open Source, Regulatory Compliance, Crisis Management, Aspect Oversight & Assessment, Security Assurance Evaluation Tools.

Level 4 System Survivability Engineering

- Goal: Demonstrate the achievement of system survivability through the management of faults and failures, sustainability processes, and RMA engineering.
- Focus Areas: Resistance, Recognition, Recovery, Reconstitution.

Level 5 System of Systems Resiliency Engineering

- Goal: Demonstrate the achievement of system of systems resiliency through the management of external interactions and dependencies, the control of distributed supervisory processes, and the practice of Next Generation software engineering.
- Focus Areas: Coordinated Recovery Time Objectives, Interoperable Information and Data Exchange, Operation Sensing and Monitoring, Digital Situation Awareness, Distributed Supervisory Control, Information and Data Recovery.

Reference:

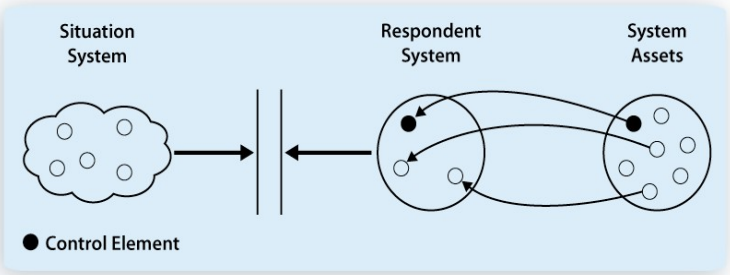
CrossTalk (2009) O'Neill, D., "*Meeting the Challenge of Assuring Resiliency Under Stress",* CrossTalk, The Journal of Defense Software Engineering, September/October 2009
http://www.crosstalkonline.org/storage/issue-archives/2009/200909/200909-ONeill.pdf

System of Systems Architecture and Engineering

A nation's critical infrastructure is composed of systems of systems. Resilience in the critical infrastructure can be reasoned about using the Systems Coupling Diagram framed by Harold "Bud"

Lawson (Figure 7). The model is composed of a Situation System, an interacting Respondent System, and Systems Assets instantiated for use as services needed by the Respondent System in its interaction with the Situation System.

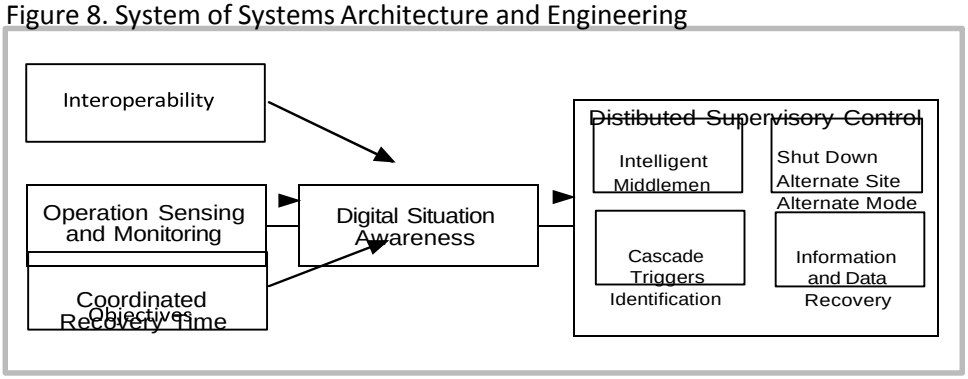
Figure 7. The System Coupling Diagram



The Systems Coupling Diagram is a template and pattern for software systems architectures of all kinds. A resilient software system architecture based on the Systems Coupling Diagram would be capable of delivering a resilient critical infrastructure system of systems.

The system of systems architecture and engineering operational concept underlying resiliency under stress is shown in Figure 8. Interoperability, operation sensing and monitoring, and coordinated recovery time objectives form the foundation for digital situation awareness. Intelligent Middlemen, response tactics, the identification of cascade triggers, and information and data recovery tactics form the ingredients for distributed supervisory control.

Figure 8. System of Systems Architecture and Engineering



In accordance with the Systems Coupling Diagram, the Software Systems Architecture for Critical Infrastructure Resilience calls for the allocation of control, function, persistent data, and assets. The architecture rules of construction associated with each factor are shown in Figure 9.

- Intelligent Middlemen in the Situation System control the Critical Infrastructure Sector transition from Normal Mode to Shut Down, Alternate Site, or Alternate Mode using the tools of the Respondent System associated with Digital Situation Awareness and Distributed Supervisory Control.
- Critical Infrastructure Sectors perform their sector functions as part of the Situation System relying on the Respondent System for Operation Sensing and Interoperability.
- Persistent Data is held and managed locally by the Critical Infrastructure Sectors relying on the Respondent System for Coordinated Recovery Time Objectives, management and control of Cascade

Triggers, and Information and Data Recovery.

- System Assets associated with security, business process continuity, and system survivability are accessed, instantiated, and consumed by the Situation System and the Respondent System. System Assets performs no control, function, or persistent data actions.

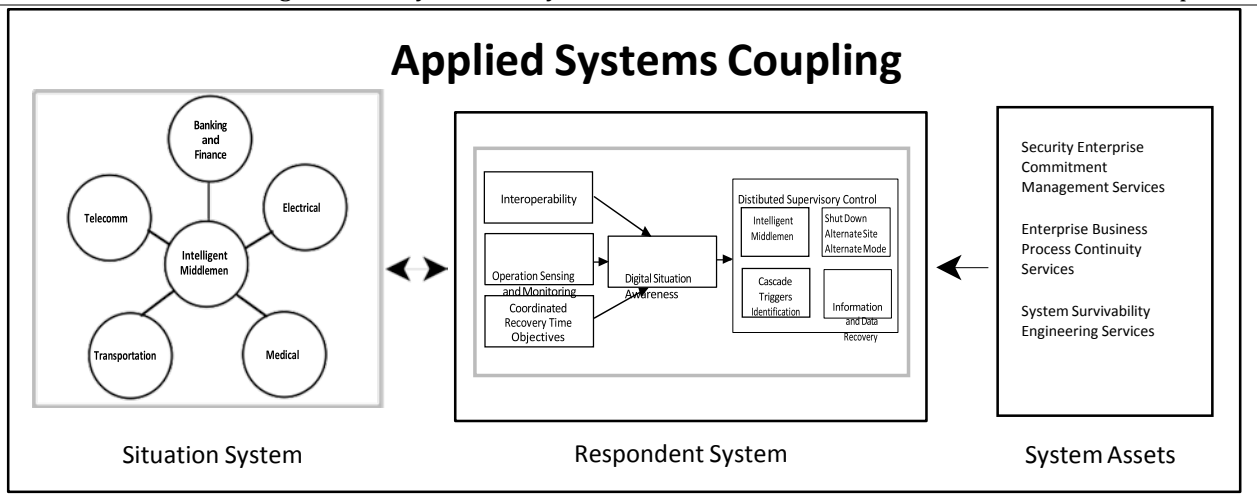
Figure 9. Rules of Construction

Factors	Situation System	Respondent System	System Assets
Control	Intelligent Middlemen • Shut Down • Alternate Site • Alternate Mode	• Digital Situation Awareness • Distributed Supervisory Control	None
Function	• Critical Infrastructure Sectors	• Operation Sensing and Monitoring • Interoperability	None
Persistent Data	Local • Critical Infrastructure Sectors	Global • Coordinated Recovery Time Objectives • Cascade Triggers • Information and Data Recovery	None
Assets	Consume • System Assets	Access • System Assets	• Enterprise Security Commitment Management Services • Enterprise Business Process Continuity Services • System Survivability Engineering Services

In accordance with the Systems Coupling Diagram, the Software Systems Architecture for Critical Infrastructure Resilience calls for the following allocation of control, functions and persistent data, and assets (Figure 10).

1. The Situation System is populated with the man-made Critical Infrastructure Sectors and the Intelligent Middlemen control node.
2. The Respondent System is populated with the Level 5 System of Systems Resiliency Engineering mission focus areas intended to interact with the Situation System and its Intelligent Middleman in anticipating, avoiding, withstanding, mitigating, and recovering from the effects of adversity under all circumstance of use.
3. The System Assets is populated with the Level 2 through 4 facilities focus areas and their services to be instantiated by the Respondent System in its interaction with Situation System and its Critical Infrastructure Sectors.

Figure 10. Applied Systems Coupling



More specifically:

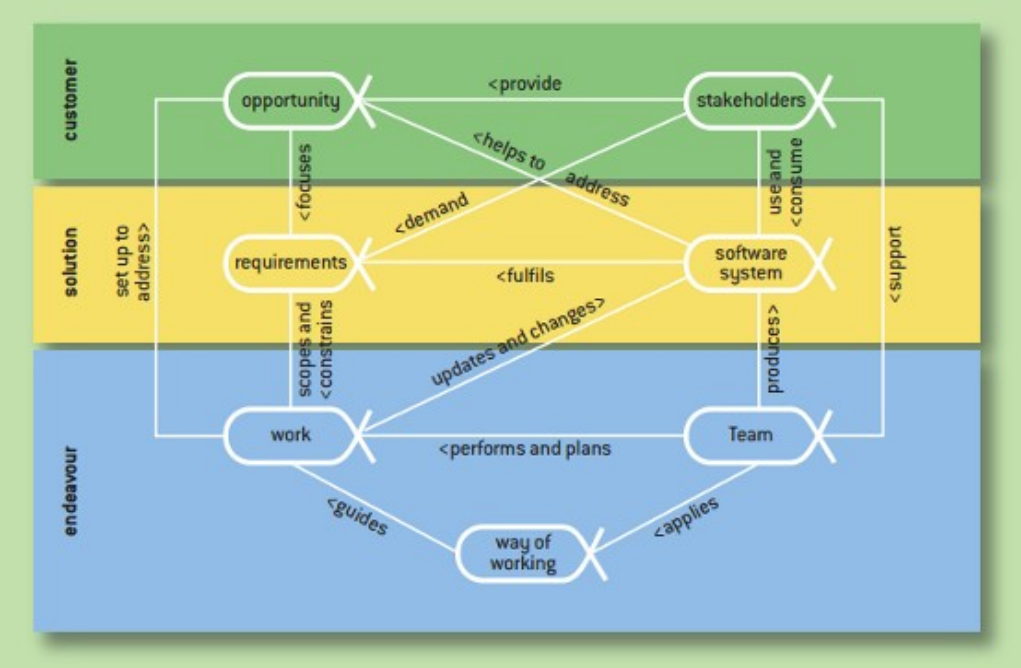
1. The critical infrastructure Situation System is composed of: Utilities and Energy, Banking and Finance, Medical Systems, Transportation, and Telecommunications as well as Public Health, Food and Agriculture, Federal Agency, Regional Response, Emergency Response, and Intelligent Middlemen control node. Each sector of the Situation System is composed of the control, functions and persistent data, and assets local to the sector.
2. The Respondent System is engineered as a system of systems architecture composed of: Coordinated Recovery Time Objectives, Interoperable Information and Data Exchange, Operation Sensing and Monitoring, Digital Situation Awareness, Distributed Supervisory Control, and Information and Data Recovery. The Situation System is composed of the control, functions and persistent data, and assets of the global system of systems.
3. The System Assets include services and facilities to be instantiated by sector: Enterprise Security Commitment Management Services, Enterprise Business Process Continuity Services, and System Survivability Engineering Services. The System Assets is composed of the facilities and service assets made available to Situation System and its sectors by the Respondent System.

Way of Working Expectations

Whether you establish criteria at the beginning of a project or not at all, there exists industrial strength objective criteria for learning the status of a project and pointing the way forward. These criteria can be found in the Software Engineering Method and Theory (SEMAT) formulation and its Essence Kernel (Jacobson, 2015), the essence and common ground of software engineering and a major Object Management Group (OMG) standards process (Figure 11).

1. The customer space is framed by a stakeholder shared vision for a well conceived value proposition for the opportunity with convincing and consequential outcomes.
2. The solution is bounded by stakeholder agreed to requirements and user stories and a software system architecture that facilitates a usable and operational software product.
3. The endeavor's work is performed by a well selected and ready team and a way of working based on established principles and foundations.

Figure11. Software Engineering Method and Theory



As the twig is bent so grows the tree. So, to get your project off on the right foot, expectations should be set and evidence should be sought on the following assertions and principles based on the following alpha state checkpoints:

1. Stakeholders are in agreement and share a vision for the project.
2. An opportunity value proposition has been established, and there is stakeholder shared vision for achieving it.
3. Requirements or user stories are coherent and acceptable, and there is stakeholder shared vision for them.
4. The software system architecture is selected and comprises a domain specific architecture to guide software system implementation, and the software system implementation is made ready and operational with no technical debt.
5. The team operates in collaboration, shares a vision for the project, and is ready to perform with respect to shared vision, software engineering process, software project management, software product engineering, operations support, and domain specific architecture processes, methods, and tools.
6. The way of working by the team has established foundations for software engineering process, software project management, software product engineering, and operations support.
7. The work is started only when all is prepared including coherent requirements and acceptable user stories, stakeholders in agreement, and an established foundation for the way of working.
8. All work products are prepared and inspected in accordance with a defined standard of excellence assuring completeness, correctness, and consistency.

Reference:

Jacobson, Ivar and Bud Lawson (2015), "*Software Engineering in the Systems Context*", College Publications, Kings College, UK, ISBN-13: 978-1848901766, October 2015, 578 pages

Integration Program Plan

The Program Plan for engineering, developing, integrating, and fielding the Critical Infrastructure Resilience System of Systems is presented here as a Work Breakdown Structure for Critical Infrastructure Resilience based on the Cleanroom Software Engineering and the SEMAT Essence Kernel Way of Working (Figure 12).

The challenge is to structure the software development plan as an incremental development with well specified design levels and incremental releases each with fine grained cost accounts, formal software inspections of design level artifacts, careful management and visibility of systems engineering "*to be determined"* items, and a relentless focus on the innovation needed to meet the challenges of resiliency.

Figure 12. Integration Program Plan

Task	Task Type	Situation System	Response System	System Assets
1.Requirements	User Stories			
2. Software System Architecture	Software System Architecture			
3. Project Planning	Increment Planning			
3.1 Design Level Planning	Increment Planning			
3.2 Incremental Development Planning	Increment Planning			
4. Design	Interface, Design, Control, and Usage			
4.1 Level 1 Design	Operating System and Middleware Environment Configuration Specification			
4.2 Level 2 Design	Intended Function and Persistent Data Specification	Sector Baselines • Intended Functions • Interface Specifications • Recovery Time Objectives	Resiliency Functions • Intended Function Specification • Persistent Data Specification	Intended Function of services and facilities
4.3 Level 3 Design	Interface and Control	Intelligent Middlemen Control Specification	Distributed Supervisor Control Specification	Defense in Depth, Business Continuity, Survivability Services Specification
4.4 Level 4 Design	Usage Specification (Arcs and Nodes Identified)	Usage Specification (Arcs and Nodes Identified)	Usage Specification (Arcs and Nodes Identified)	Usage Specification (Arcs and Nodes Identified)
4.5 Level 5 Design	Usage Modeling (Frequency Annotations on Arcs)	Usage Modeling (Frequency Annotations on Arcs)	Usage Modeling (Frequency Annotations on Arcs)	Usage Modeling (Frequency Annotations on Arcs)
4.6 Level 6 Design	Statistical Testing Design			
4.7 Level 7 Design	Acceptance Test Design			
5. Development	Procedure Development			

5.1 Operating Environment	Operating System and Middleware Environment Configuration Setup			
5.2 Incremental Development	Increment Planning	Procedure Development of Intelligent Middlemen Control • Stepwise Refinement of Intended Functions • Correctness Verification	Procedure Development of Resiliency Functions • Stepwise Refinement of Intended Functions • Correctness Verification	Procedure Development of services and facilities • Stepwise Refinement of Intended Functions • Correctness Verification
6. Test	Statistical Testing and Certification			
6.1 Statistical Testing				
6.2 Certification				

Resilience Assurance and Risk Calculation

Risk and value go hand in hand. It is necessary to take risk in order to exploit opportunities (DeMarco and Lister, 2003). A common approach is to put a big toe in the water by making a minimum commitment and hope to get lucky. This is a low commitment, high risk tactic (Figure13). The risk here is that the outcome being sought may be highly uncertain unless a sufficient commitment of resource is applied. Another approach is to take the plunge by making a full commitment of resources and sticking with it until it produces results or the value proposition is reevaluated. This is a high commitment, low risk strategy.

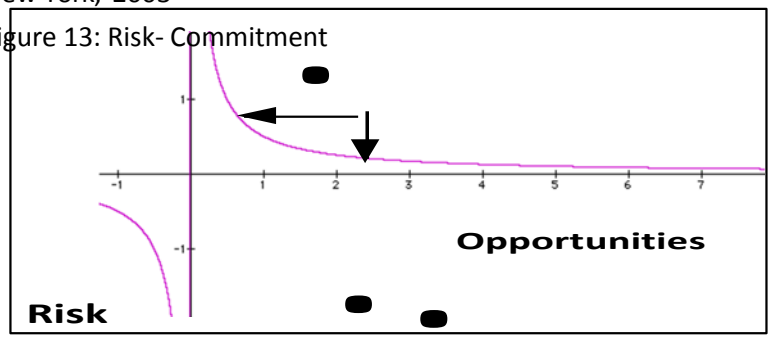
There is evolving an overemphasis and dependence in both the acquisition and development communities on process conformance, standards compliance, and risk adversity. Achieving innovation requires a paradigm shift towards creativity, increased experimentation, and risk taking.

Improving the attractiveness of opportunities is an important dimension of competitiveness. Higher levels of risk can be offset by higher levels of commitment (resources like cost, schedule, and staff). But it is not simply an issue of resources. Achieving value requires seeking out and taking prudent and calculated risk. While it is necessary to take risk to obtain value, simply taking risk does not in itself yield value. Readiness factors within the prescription for success are also involved including software process maturity, application domain expertise, technical architecture, and way of working.

Reference:

DeMarco, T. and Lister, T. (2003) "*Waltzing With Bears"*, Dorset House Publishing Co., Inc., New York, New York, 2003

Figure 13: Risk- Commitment



Commitment

In the pursuit of critical infrastructure resilience, preparation for calculating resilience earned value and resilience risk begins by focusing on the definition of resilience as the goal. Restatement of goals and objectives as affirmative assertions initiates a rigorous proof process sequence composed of bold assertions, convincing arguments, and supporting evidence.

DEFINITION OF RESILIENCE

The preferred definition of resilience is the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity whether natural or man made under all circumstances of use.

PREPARATION

1. Identify the steps in assuring the operations and the risks associated with the following:
    a. Anticipation

b. Avoidance
c. Withstanding
d. Minimize
e. Recovery

2. Identify the effects of adversity associate with:
   a. Natural events
   b. Man made incidents

3. Identify all circumstances of

use. ASSERTION
The resilience of the critical infrastructure is assured.

ARGUMENTS
1. The risk associated with the resiliency operations of anticipation, avoidance, withstanding, minimizing, and recovering has been assessed and found acceptable.
2. All anticipated effects of adversity associated with the effects of adversity including natural events and mad made incidents have been identified and considered.
3. All anticipated circumstances of use have been identified and considered.

EVIDENCE
1. Convincing evidence of context and culture harmonization exists.
2. Convincing evidence of intelligent middlemen readiness exists.
3. Convincing evidence of resiliency maturity exists.
4. Convincing evidence of system of systems architecture adoption exists.
5. Convincing evidence of integration engineering program planning exists.
6. Convincing evidence of a defined way of working exists.
7. Convincing evidence of supply chain risk management assurance against counterfeiting and tampering exists.
8. Convincing evidence of cyber security strategy and tactics exists to assure the operations associated with anticipation, avoidance, protection, withstanding, minimize, and recovery.

A Critical Infrastructure Resilience Assurance Assessment and Risk Calculation Worksheet (Figure 14) is used to compile the assurance evidence element scores of 46 risk indicators for each of five industry sectors. Each indicator is scored 1 (low) to 5 (high). Both the assurance evidence elements and the industry sectors are assigned weights of 1-5. This Critical Infrastructure Resilience dashboard is intended to shine a spotlight on resilience risk and earned value in order to reveal gaps, suggest vulnerabilities, and point the way forward for participating industry sectors.

Figure 14. Resilience Assurance Assessment and Risk Calculation Worksheet

Assurance Evidence	Risk Indicator (Score1-5)	Electrical Sector	Telecom Sector	Banking & Finance	Transport. Sector	Medical Sector
Culture and Context Harmonization	• Formality of domain engineering • Strong code management • Workforce control • Government control • Harmonization of expectations • Technical debt elimination • Cascade trigger anticipation • Software product sourcing exposure • Supply chain risk management assurance • Cyber security strategy and tactics					
Intelligent Middlemen Readiness	• Experienced and educated • Experienced as Chief Engineer • Boundary spanner • State transition management • Focus on resilience goal					
Resiliency Maturity	• L2 Security in depth • L3 Business process continuity • L4 Survivability and availability • L5 System of system resiliency					
System of Systems Architecture Adoption	• Situation System • Respondent System • System Assets					
Integration Engineering Program Plan	• Engineering • Developing • Integrating • Fielding					
Way of Working	• Stakeholders in agreement • Opportunity value proposition • Acceptable requirements • Software system architecture • Team collaboration • Foundations for way of working • Work is started • Work products are inspected					
Resilience Assurance and Risk Calculation	• Preparation • Assertions • Arguments • Evidence • Resiliency assurance • Risk Calculation					
Cyber Security Strategy and Tactics	• Cyber strategy policy in place • Anticipation tactics ready • Protection tactics ready • Detection tactics ready • Attribution tactics ready • Counter measure tactics ready					

The resilience earned value calculation measures the degree to which the resilience value proposition is being achieved in each industry sector and resilience risk highlights areas needing attention. Resilience risk is unattended value or opportunities to improve resilience that are known but not yet taken.

- Resilience Earned Value := Weighted Example / Weighted Maximum
  Where: weights are assigned industry sectors and integrating elements and all indicators are scored as 5's

Weighted Minimum	Weighted Example	Weighted Maximum
2499	8101	12,495

- Resilience Risk := (1-Resilience Earned Value)

- Resilience Earned Value: Weighted Example / Weighted Maximum = 8101/12495 = 0.64833
- Resilience Risk: (1- Resilience Earned Value) = (1-8101/12495) = 0.35166

Figure 15 details the assurance evidence for a weighted example along with resilience risk and earned value calculation.

Figure 15. Resiliency Risk and Earned Value Calculation

Assurance Evidence (Weighted Example)	Risk Indicator (Score 1-5)	Indicator Weight	Electrical Sector	Telecom Sector	Banking & Finance Sector	Transport. Sector	Medical Sector	Weighted Score	Risk	Earned Value
			5	**4**	**3**	**3**	**2**			
A. Culture and Content Harmonization		**4**	800	624	468	312	160	2364	0.304706	0.6952941
B. Intelligent Middlemen		**2**	240	292	144	84	48	708	0.167588	0.8329412
C. Resiliency Maturity		**5**	325	260	240	210	140	1175	0.3088235	0.6911765
D. System of Systems Architecture Adoption		**5**	200	160	129	105	70	655	0.4862745	0.5137256
E. Integration Engineering		**2**	130	104	72	60	36	402	0.4088235	0.5911766
F. Way of Working		**3**	420	336	333	234	132	1455	0.2867647	0.7132353
G. Resilience Assurance and Risk Calculation		**2**	170	136	102	78	52	538	0.472549	0.527451
H. Cyber Security Strategy and Tactics		**3**	240	192	162	126	84	804	0.4745098	0.5254902
Total Indicators	723		2525	2004	1641	1209	722	8101	0.3516607	0.6483393

Figure 16 provides a completed worksheet of a weighted example.

Figure 16. Worksheet Weighted Example

Assurance Evidence	Risk Indicator (Score 1	Indicator Weig	Electrical Sec	Telecom Sectc	Banking & Fi	Transportatio	Medical Sect	Weighted Sc	Indicator Scc	Earned Value	**Risk**
(Weighted Example)			Sector Weight	Sector Weight	Sector Weigh	Sector Weigh	Sector Weight				
A. Culture and Content Harmonization		**4**	**5**	**4**	**3**	**3**	**2**				
1. Formality of domain engineering	17		3	4	4	3	3		68		
2. Strong code management	18		4	4	4	3	3		72		
3. Workforce control	20		5	5	5	3	2		80		
4. Government control	21		5	5	5	4	2		84		
5. Harmonization of expectations	20		5	5	5	3	2		80		
6. Technical debt elimination	16		5	4	3	2	2		64		
7. Cascading and propagating triggers	15		4	4	3	2	2		60		
8. Software sourcing exposures	12		3	3	3	2	1		48		
9. Supply Chain Risk Management Assu	11		3	2	3	2	1		44		
10. Cyber Security Strategy and Tactics	14		3	3	4	2	2		56		
Subtotal			800	624	468	312	160	2364		0.69529412	**0.30470588**
B. Intelligent Middlemen Readiness		**2**									
1. Experienced and educated	18		4	4	4	3	3		36		
2. Experienced as Chief Engineer	19		5	5	5	2	2		38		
3. Boundary spanner	20		5	5	5	3	2		40		
4. State transition management	21		5	5	5	3	3		42		
5. Focus on resilience goal	20		5	5	5	3	2		40		
Subtotal			240	192	144	84	48	708		0.83294118	**0.16705882**
C. Resiliency Maturity		**5**									
1. L2 Security in depth	10		2	2	2	2	2		50		
2. L3 Business process continuity	21		4	4	5	4	4		105		
3. L4 Survivability and availability	19		4	4	5	3	3		95		
4. L5 System of system resiliency	20		3	3	4	5	5		100		
Subtotal			325	260	240	210	140	1175		0.69117647	**0.30882353**
D. System of Systems Architecture Adoption		**5**									
1. Situation System	18		4	4	4	3	3		90		
2. Respondent System	10		2	2	2	2	2		50		
3. System Assets	10		2	2	2	2	2		50		
Subtotal			200	160	120	105	70	655		0.51372549	
E. Integration Engineering		**2**									
1. Engineering	17		4	4	3	3	3		34		
2. Developing	14		3	3	3	3	2		28		
3. Integration	13		3	3	3	2	2		26		
4. Fielding	13		3	3	3	2	2		26		
Subtotal			130	104	72	60	36	402		0.59117647	**0.40882353**
F. Way of Working		**3**									
1. Stakeholder in agreement	18		4	4	5	3	2		54		
2. Opportunity value proposition	19		4	4	5	3	3		57		
3. Acceptable requirements	19		4	4	5	3	3		57		
4. Software system architecture	17		3	3	5	3	3		51		
5. Team collaboration	18		3	3	5	4	3		54		
6. Foundations for way of working	14		3	3	4	2	2		42		
7. Work is started	17		3	3	4	4	3		51		
8. Work products are inspection	19		4	4	4	4	3		57		
Subtotal			420	336	333	234	132	1455		0.71323529	**0.28676471**
G. Resilience Assurance and Risk Calculation		**2**									
1. Preparation	21		5	5	5	3	3		42		
2. Assertions	18		4	4	4	3	3		36		
3. Arguments	13		3	3	3	2	2		26		
4. Evidence	10		2	2	2	2	2		20		
5. Resilience assurance	10		2	2	2	2	2		20		
6. Risk calculation	5		1	1	1	1	1		10		
Subtotal			170	136	102	78	52	538		0.52745098	**0.47254902**
H. Cyber Security Strategy and Tactics		**3**									
1. Cyber strategy policy in place	18		4	4	4	3	3		54		
2. Anticipation tactics ready	11		2	2	3	2	2		33		
3. Protection tactics ready	15		3	3	3	3	3		45		
4. Detection tactics ready	15		3	3	3	3	3		45		
5. Attribution tactics ready	11		2	2	3	2	2		33		
6. Counter measure tactics ready	8		2	2	2	1	1		24		
Subtotal			240	192	162	126	84	804		0.5254902	**0.4745098**
Total Indicators	723		2525	2004	1641	1209	722	8,101		0.64833934	**0.35166066**

NEXT STEPS

For best results, the value proposition for resilience is based on the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity whether natural or man made under all circumstances of use. Instead, the Government is settling for the operations of withstanding, minimizing, and recovering. Why is this a problem? The most consequential threat to resilience lies in the cascading and propagating triggers that lie hidden in the complexity of critical sector interactions and dependencies inherent in the system of systems that make up the Critical Infrastructure. Without anticipation and avoidance, cascade triggers are left unattended.

The critical infrastructure resilience issues associated with context and culture comprise the principal integration engineering challenges to be addressed by the resilience integrator and the Intelligent Middlemen. The role of the resilience integrator is to press for higher resilience earned value scores by addressing the resilience issues and adopting the integrating element prescriptions. Figure 17 suggests the connection between the resilience issues discussed and the integrating elements specified and highlights the areas of best opportunities for boosting resilience earned value and reducing resilience risk by eliminating unattended value.

Figure 17. Resilience Issues and Integrating Elements

Resilience Issues/ Integrating Elements	Intelligent Middlemen	Resiliency Maturity	System of Systems Architecture	Integration Engineering Plan	Way of Working	Resilience Assurance and Risk Management
Formality within an architectural framework	*		*		*	*
Strong code management practice	*				*	*
Strong industry sector control over workforce	*				*	*
Strong government control over industry sectors	*	*	*			*
Expectation of trust, loyalty, and satisfaction	*					*
Technical debt elimination	*			*	*	*
Cascade trigger anticipation	*	*	*			*

Software product sourcing exposure	*			*	*	*
Supply chain risk management assurance	*			*	*	*

What is the Next Move?

The overall demonstration of the mission to achieve Critical Infrastructure Resilience is being initiated in several parts including the composition of a User Story and subject of earlier work; the assessment of industry sector Resiliency Maturity, compatibility of industry sector context and culture, industry sector Technical Debt, and industry sector Intelligent Middleman readiness; specification of the Critical Infrastructure Resilience System of Systems Architecture Respondent System; and a Program Plan for engineering, developing, integrating, and fielding the Critical Infrastructure Resilience System of Systems Respondent System in terms of a Way of Working.

The state of the Critical Infrastructure Resilience System of Systems Respondent System is shown here with the current state of progress in italics type and next steps underlined:

- Stakeholder- **recognized,** represented, involved, in agreement, satisfied with deployment, satisfied in use
- Opportunity- **identified**, **software needed**, value established, viable, addressed, benefit accrued
- Requirements- **conceived, bounded, coherent,** acceptable, addressed, fulfilled
- Software System- **architecture selected,** demonstrable, usable, ready, operational, retired
- Team- selected, formed, collaborating, performing, adjourned
- Way of Working- **principles established, foundations established,** in use, in place, working well, retired
- Work- initiated, prepared, started, under control, concluded, closed
- Work product- identified, produced, inspected, complete, correct, consistent, value add

Recap

To what extent is critical infrastructure resilience a strategic imperative? The principles, foundations, and elements of Integration Engineering in the pursuit of Critical Infrastructure Resilience set the table for research in practice and pave the way for the role of a Critical Infrastructure Resilience Integrator as follows:

1. The harmonization of the context and culture of industry sectors in the critical infrastructure domain.
2. The defined role and job description of the Intelligent Middleman as the traffic cop for harmonious cooperation among industry sectors.
3. The order and utility of the focus areas in the Resiliency Maturity Framework.
4. The application of model-based Systems Architecture and the Systems Coupling Diagram with its Situation System, Respondent System, and System Assets in the Critical Infrastructure Resilience System of Systems Architecture along with specified architecture rules of construction spanning control, function, persistent data, and assets.
5. The utility of the Software Engineering Method and Technology (SEMAT) Essence Kernel Way of Working in bridging the gap between managers and technical practitioners among industry sectors in Resilience Integration Program Planning.
6. The public policy imperative to enhance situation awareness through information sharing and unfreeze the impasse by indemnifying private industry sector participants.

To what extent is there the political will to pursue a Critical Infrastructure System of Systems based

upon the following?

- Is there harmonization of Context and Culture?
- Is there capability readiness of Intelligent Middlemen?
- Is there advancement of Resiliency Maturity?
- Is there adoption of a System of Systems Architecture?
- Is there execution of an Integration Program Plan?
- Is there advancement of Public Policy Imperatives?
- Is there a common Way of Working among the industry sectors?

A Demonstration of Political Will

Appendix B defines a Pilot Program of Government leadership in Cyber Security, one that would represent a concrete and actionable achievement by the Commission on Enhancing National Cyber Security. Not just a problem diagnosis, this program takes a bold step towards a problem solution. Based on an architecture of resilience, the Pilot Program would provide convincing evidence of the political will, technical leadership, innovative thinking , and public/private collaboration needed to meet one of the most consequential challenges of Cyber Security facing the nation and would do so on a milestone schedule set by the Cyber Commission's period of performance scheduled to conclude on December 1, 2016.

The Pilot Program represents the first increment of a Critical Infrastructure model of operational resilience, one that emphasizes data flow, interfaces, state transitions, and interactions among industry sectors. As an artifact of infrastructure itself, the model is intended to be refined and extended to reflect an understanding of the operational complexities among industry sectors emerges, potential cascade triggers are anticipated and identified, intelligent distributed supervisory control tactics are formulated to avoid their effects, and the need and opportunity for additional digital situation awareness. The result sought is an operationally resilient Critical Infrastructure model that will guide the integration engineering of industry sector systems into the Situation System, Respondent System, and System Assets of the system of systems architecture.

References:

Bank (2001) *A Glossary of Terms in Payment and Settlement Systems*, Committee on Payment and Settlement Systems, Bank for International Settlements, 2001.

CyLab (2008), O'Neill, D., "*Inside Track to Offshore Outsourcing Using the Trusted Pipe™: What Global Enterprises Look For in Offshore Outsourcing",* Making the Business Case for Software Assurance Workshop, Carnegie Mellon CyLab, Pittsburgh, PA, September, 2008, pages 59-75

CrossTalk (2003) O'Neill, D., "*Introducing Global Software Competitiveness"*, CrossTalk, The Journal of Defense Software Engineering, Online Articles, October 2003 http://www.crosstalkonline.org/storage/issue-archives/2003/200310/200310-ONeill.pdf

CrossTalk (2009) O'Neill, D., "*Meeting the Challenge of Assuring Resiliency Under Stress",* CrossTalk, The Journal of Defense Software Engineering, September/October 2009
http://www.crosstalkonline.org/storage/issue-archives/2009/200909/200909-ONeill.pdf

CrossTalk (2011) O'Neill, D., "*Cyber Strategy, Analytics, and Tradeoffs: A Cyber Tactics Study",* CrossTalk, The Journal of Defense Software Engineering, September/October 2011
http://www.crosstalkonline.org/storage/issue-archives/2011/201109/201109-ONeill.pdf

CrossTalk (2012) O'Neill, D., *Extending the Value of the CMMI to a New Normal",* CrossTalk, The Journal of Defense Software Engineering, January/February 2012
http://www.crosstalkonline.org/storage/issue-archives/2012/201201/201201-ONeill.pdf

CrossTalk (2014.1) O'Neill, D., *"Software Assurance, Trustworthiness, and Rigor*", CrossTalk, The Journal of Defense Software Engineering,

September/October 2014 http://www.crosstalkonline.org/storage/issue-archives/2014/201409/201409-ONeill.pdf

CrossTalk (2014.2) O'Neill, D.,*"Software and Supply Chain Risk Management Assurance Framework",* CrossTalk, The Journal of Defense Software Engineering, March/April 2014
http://www.crosstalkonline.org/storage/issue-archives/2014/201403/201403-ONeill.pdf

Defense AT&L (2013) O'Neill, D., *"Technical Debt in the Code: Cost to Software Planning",* Defense Advanced Technology and Logistics (DAT&L) Magazine, March-April 2013
http://www.dau.mil/pubscats/ATL%20Docs/Mar_Apr_2013/O%27Neill.pdf

Defense AT&L (2015), O'Neill, D., *"Software 2015: Situation Dire"*, Defense Advanced Technology and Logistics (DAT&L) Magazine, May-June 2015 http://www.dau.mil/publications/DefenseATL/DATLFiles/May-Jun2015/O'Neill.pdf

DeMarco, T. and Lister, T. (2003) "*Waltzing With Bears"*, Dorset House Publishing Co., Inc., New York, New York, 2003

EMP (2004) *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, Volume 1: Executive Report, 2004.

FED et al (2002) *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System,* The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, September 5, 2002.

IBM SJ (1980) Mills, H.D., O'Neill, D., Linger, R.C., Dyer, M., Quinnan, R.E. (1980) "*The Management of Software Engineering*", IBM Systems Journal (SJ), Volume 19, Number 4, 1980, pages 414-477
http://www.research.ibm.com/journal/sj/

Jacobson, Ivar and Bud Lawson (2015), "*Software Engineering in the Systems Context*", College Publications, Kings College, UK, ISBN-13: 978-1848901766, October 2015, 578 pages

JSS (1983), O'Neill, D., "*Integration Engineering Perspective*", The Journal of Systems and Software (JSS), 3, 77-83, 1983 http://www.sciencedirect.com/science/article/pii/0164121283900067

Appendix A: Convincing Evidence Of Resiliency Integration Engineering Convincing Evidence of Context and Culture Harmonization

1. Formality within an architectural framework facilitates the imposition of distributed supervisory control, interoperability, and operation sensing and monitoring protocols.
2. Strong code management practices facilitate reconfiguration and reconstitution.
3. Exercising strong control over the workforce facilitates business continuity and survivability.
4. Exercising strong government control facilitates compliance for the benefit of the commons at the expense of initiative for the self-interest.
5. The diverse industry sector expectations of trust, loyalty, and satisfaction must be respected, blended, and harmonized.
6. Technical Debt must be eliminated.
7. Cascading and propagating triggers must be anticipated, avoided, and minimized.
8. Industry sector software sourcing exposures must be understood and managed.
9. Supply chain risk management assurance must be adopted.
10. Cyber security strategy policy decisions and defined tactics must be assured.

Convincing Evidence of Intelligent Middlemen Readiness

1. The Intelligent Middleman must be educated, trained, and in possession of the broad gauge experience to fill the role of Chief Critical Infrastructure Resilience Architecture and Operations Engineer.
2. As Chief Engineer, the Intelligent Middleman must be educated and trained in the prerequisite essentials of both systems engineering and software engineering and have experience in how things are built and how things are used from architecture through operations.
3. As a boundary spanner, the Intelligent Middleman must understand and be capable of planning and exercising command and control of the Critical Infrastructure under stress.
4. Specifically, the Chief Engineer must mange the state transitions associated with its electrical grid and data transmission infrastructure, interoperability and information sharing protocols, Cyber Security framework, law enforcement and emergency services, sector coordinated recovery time objectives, cascade triggers, digital situation awareness, information and data recover protocols, distributed supervisory command and control protocols, and supply chain logistics and risk management.
5. The Intelligent Middleman must maintain the foremost focus on the goal of anticipating, avoiding, withstanding, mitigating, and recovering from the effects of adversity whether natural or manmade under all circumstances of use.

Convincing Evidence of Resiliency Maturity

1. Level 2 Security in Depth
2. Level 3 Business Process Continuity
3. Level 4 Survivability and Availability
4. Level 5 System of System Resiliency

Convincing Evidence of System of Systems Architecture Adoption

1. The Situation System is populated with the man-made Critical Infrastructure Sectors and the Intelligent Middlemen control node.
2. The Respondent System is populated with the Level 5 System of Systems Resiliency Engineering mission focus areas intended to interact with the Situation System and its Intelligent Middleman in anticipating, avoiding, withstanding, mitigating, and recovering from the effects of adversity under all circumstance of use.
3. The System Assets is populated with the Level 2 through 4 facilities focus areas and their services to be instantiated by the Respondent System in its

interaction with Situation System and its Critical Infrastructure Sectors.

Convincing Evidence of an Integration Engineering Program Plan

Planning for engineering, developing, integrating, and fielding the Critical Infrastructure Resilience System of Systems contains a Work Breakdown Structure for Critical Infrastructure Resilience based on the Cleanroom Software Engineering and the SEMAT Essence Kernel Way of Working.

Convincing Evidence of A Way of Working

1. Stakeholders are in agreement and share a vision for the project.
2. An opportunity value proposition has been established, and there is stakeholder shared vision for achieving it.
3. Requirements or user stories are coherent and acceptable, and there is stakeholder shared vision for them.
4. The software system architecture is selected and comprises a domain specific architecture to guide software system implementation, and the software system implementation is made ready and operational with no technical debt.
5. The team operates in collaboration, shares a vision for the project, and is ready to perform with respect to shared vision, software engineering process, software project management, software product engineering, operations support, and domain specific architecture processes, methods, and tools.
6. The way of working by the team has established foundations for software engineering process, software project management, software product engineering, and operations support.
7. The work is started only when all is prepared including coherent requirements and acceptable user stories, stakeholders in agreement, and an established foundation for the way of working.
8. All work products are prepared and inspected in accordance with a defined standard of excellence assuring completeness, correctness, and consistency.

Convincing Evidence of Supply Chain Risk Management Assurance

1. Preparations have been made to carry out Supply Chain Risk Management Assurance.
2. Assertions pertaining to Supply Chain Risk have been made, for example, with respect to tampering and counterfeit parts.
3. Convincing arguments in support of Supply Chain Risk assertions have been set forth.
4. Convincing evidence to back up the arguments is available.
5. Resilience assurance assessments are being conducted.
6. Calculated risks are being made as part of Supply Chain Risk Management.

Convincing Evidence of Cyber Security Strategy and Tactics

1. A Cyber Strategy is a policy of defined tradeoffs is in place.
2. Cyber Tactics for anticipation are ready for deployment.
3. Cyber Tactics for protection are ready for deployment.
4. Cyber Tactics for detection are ready for deployment.
5. Cyber Tactics for attribution are ready for deployment.
6. Cyber Tactics for counter measures are ready for deployment.

Appendix B: Convincing Evidence of the Presence of Political Will to Pursue a Resilient Critical Infrastructure System of Systems

Milestone Schedule	Pilot Program Tasks
April 2016	Select Critical Infrastructure industry sectors to pilot and identify named representative for each industry sector
May 2016	Obtain shared vision on the value proposition and integration engineering approach and produce an operational concept of industry sector interactions and state transitions.
June 2016	Model the system of systems architecture selected, demonstrate the model, and exercise it with an eye on industry sector interfaces, state transitions, and cascade trigger identification and mitigation.
July 2016	Select the team in each industry sector to collaborate and implement the Situation System.
July 2016	Select the team to collaborate and implement the Respondent System behavior associated with digital situation awareness and distributed supervisory control
July 2016	Select the team to collaborate and implement System Assets needed for defense in depth, business process continuity, and survivability.
August 2016	Obtain shared vision among the teams on the way of working based on principles and foundations established.
August 2016	Initiate the work.
September 2016	Identify work products to be produced and inspected for completeness, correctness, consistency, and achievement of value add.
October 2016	Assess resilience assurance of the Critical Infrastructure using the resiliency risk and earned value calculation spreadsheet and worksheet.
November 2016	Pilot Program Initial Operating Capability needed to model the effectiveness of shutdown, minimum essential function, coordinated recovery time objectives, and cascade triggers.
December 2016	Pilot Program increment concluded.

14419 words

YouTube

Title: Critical Infrastructure Resilience Integration Engineering
https://youtu.be/37GnHe6Zo2w
31:50 minutes

Description
The critical infrastructure is the industrial base on which the competitiveness and security of the nation are dependent. The current state of the nation's critical infrastructure is at risk. The Internet has become the central nervous system of the nation both private and public. The nation's critical infrastructure continues to be vulnerable to natural disasters and cascading Cyber Security attacks. In fact, software has become the "*critical infrastructure within the critical infrastructure*" as noted by Dr. Alan Salisbury at the Second National Software Summit (NSS2) in 2004[1].

The role of the Critical Infrastructure Resilience Integration Engineering is being described in five parts:
1. An assessment of the context and culture for industry sectors.
2. An assessment of the readiness to fulfill the Intelligent Middleman job description for each industry sector.
3. An assessment of the Resiliency Maturity Framework for industry sectors.
4. Specification of the Critical Infrastructure Resilience System of Systems Architecture.
5. Preparation of a Program Plan for engineering, developing, integrating, and fielding the Critical Infrastructure Resilience System of Systems in terms of a Way of Working.

Tags:
harmonization context and culture, elimination of Technical Debt, Capability of Intelligent Middlemen, advancement of Resiliency Maturity, adoption of system of systems architecture, execution of Integration Program Plan, advancement of Public Policy imperative, harmonization of industry sectors, Intelligent Middlemen, Resilience Maturity Framework, System of Systems Architecture, Way of Working, Integration Engineering

[1] Jacobson, Ivar and Bud Lawson (2015), *"Software Engineering in the Systems Context",* College Publications, Kings College, UK, ISBN-13: 978-1848901766, October 2015, 578 pages

Don O'Neill

Don O'Neill is a seasoned software engineering manager and technologist currently serving as an independent consultant. Following his twenty-seven year career with IBM's Federal Systems Division, Mr. O'Neill completed a three-year residency at Carnegie Mellon University's Software Engineering Institute (SEI) under IBM's Technical Academic Career Program and has served as an SEI Visiting Scientist.

As an independent consultant, Mr. O'Neill conducts defined programs for managing strategic software improvement. These include implementing an organizational Software Inspections Process, directing the National Software Quality Experiment, implementing Software Risk Management on the project, conducting the Project Suite Key Process Area Defined Program, conducting Team Innovation Management training, and conducting Global Software Competitiveness Assessments. Each of these programs includes the necessary practitioner and management training. As an expert witness, he provides testimony on the state of the practice in developing and fielding large- scale industrial software and the complex factors that govern their outcome with respect to competitiveness, security, and trustworthiness.

In his IBM career, Mr. O'Neill completed assignments in management, technical performance, and marketing in a broad range of applications including space systems, submarine systems, military command and control systems, communications systems, and management decision support systems. He was awarded IBM's Outstanding Contribution Award three times:

1. Software Development Manager for the Global Positioning (GPS) Ground Segment (500,000 source lines of code) and a team of 70 software engineers within a $150M fixed price program.
2. Manager of the FSD Software Engineering Department responsible for the origination of division software engineering strategies, the preparation of software management and engineering practices, and the coordination of these practices throughout the division's software practitioners and managers.
3. Manager of Data Processing for the Trident Submarine Command and Control System Engineering and Integration Project responsible for architecture selections and software development planning (1.2M source lines of code).

As an inventor, Mr. O'Neill has two patents pending. One, trademark registered Trusted Pipe™, is entitled *"Business Management and Procedures Involving Intelligent Middleman"*, an apparatus and method for the inside track to offshore outsourcing. The other, trademark registered Smart Pipe™, is entitled *"Business Management and Procedures Involving a Smart Pipe of Tiered Innovation Management Teams"*, an apparatus and method for harvesting ideas as intellectual property from knowledge workers on projects, whether onshore or offshore.

Mr. O'Neill served on the Executive Board of the IEEE Software Engineering Technical Committee and as a Distinguished Visitor of the IEEE. He is a founding member of the Washington DC Software Process Improvement Network (SPIN) and the National Software Council (NSC) and served as the President of the Center for National Software Studies (CNSS) from 2005 to 2008. He was a contributing author of "*Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness",* a report on the Second National Software Summit. Mr.
O'Neill has served as a reviewer of National Science Foundation (NSF) software engineering research proposals and has served as a member of the NIST Software Assurance Metrics and Tool Evaluation

(SAMATE) Advisory Committee (2006-2008). He has authored Business Case articles for the CERT Build Security In (BSI) web site. He has lectured on global software competitiveness, innovation, and outsourcing at the National Defense University (NDU) and on Software Risk Management at George Washington University (GWU) and San Diego State University.

His current research is directed at public policy strategies for reconciling privacy and security stresses; deploying resiliency in the nation's critical infrastructure; disruptive game changing fixed price contracting tactics to achieve DOD austerity; smart and trusted tactics and practices in Supply Chain Risk Management Assurance; a defined Software Clean Room Method for transforming a proprietary system into a Clean System devoid of proprietary information, copyrighted material, and trade secrets and confirming, verifying, and validating the results, and a constructive approach to sequencing the transition of SEMAT Essence Kernel Alpha states with an eye to pinpointing the risk triggers that threaten success and lead to the accumulation of technical debt.

Mr. O'Neill is an active speaker on software engineering topics and has numerous publications to his credit. He has a Bachelor of Science degree in mathematics from Dickinson College in Carlisle, Pennsylvania.

® Trusted Pipe is registered with the U.S. Patent and Trademark Office by Don O'Neill.

® Smart Pipe is registered with the U.S. Patent and Trademark Office by Don O'Neill.

http://www.linkedin.com/in/oneilldon

April 17, 2016

To: Chair and Vice Chair, Commission on Enhancing National Cyber Security
cc: Kiersten Todt, Cyber Commission Executive Director

Subject: Cyber Commission Kickoff Followup: A Demonstration of Political Will and Technological Leadership to Protect Our Cyberspace Strategic Advantage

Dear Messrs. Donilon and Palmisano,

I appreciate the opportunity to have offered my comments to the Cyber Commission at its kickoff meeting on April 14, 2016 at the Department of Commerce in Washington, DC. I am following up with the Cyber Commission due to a sense of urgency on the stubborn issue of Critical Infrastructure resilience, which I spoke about, and the opportunity to build momentum that will carry forward into the next Administration.

INTERNET UNDER SIEGE

Cyber Security is the existential threat of our times. A sensible, risk adverse manager with data and information the organization cannot afford to lose under any circumstances would be advised not to entrust it to the Internet. The U.S. Navy has already adopted such a policy for critical circumstances. The sensible risk adverse manager may choose to risk some information and data to the Internet but will do so provided it is encrypted and access requires three facto authentication. Clearly the Internet is under siege. While some may argue that Cyber Security is a marathon, they also need to know that adversaries in the race are running at sprinter's speed.

TOPICS FOR DELIBERATION

Asking the question, *"Do the topics selected for Cyber Commission deliberation adequately frame the Cyber Security challenge?"* The straightforward answer, *"The topics suggested resemble a laundry list or window dressing."* The topics suggest a formulaic awareness and change management tilt without attention to the underlying science and engineering foundations needed.

Hard problems do not give way to easy solutions. Even as a laundry list, the topics fail the test of completeness since they contain no mention of the need to establish Cyber Security theory and practice foundations along the lines of State of the Art (SOA) and State of the Practice (SOP). Despite this deficit, several topics on the list rely on the existence of such a body of knowledge as principal prerequisites including Federal Roles, Cyber Workforce, and International Norms. No small thing, this single point of failure dooms these tasks from the start with a promise of incomplete or invalid results.

CRITICAL INFRASTRUCTURE OPPORTUNITY

It is recognized that Critical Infrastructure resilience is a hard problem, perhaps an intractable one. This topic should be singled out by the Cyber Commission for immediate action in order to demonstrate that the Government possesses the political will and will make the technological leadership commitment to defend the nation's strategic advantage in Cyberspace and to do so with the necessary sense of urgency in tackling this hard problem in recognition of the fact that without a solution it's literally lights out. In short, we have an opportunity to act now and with a sense of urgency to take a concrete, incremental step towards addressing a consequential issue with a bold action designed to be sustainable.

Just what action should be taken? The action should be immediate and should begin with the intention to deliver consequential results while the Cyber Commission is in session. There is the need then to generate sufficient momentum and the credible early results that will ensure the initiative will carry over into the next Administration and beyond.

SOLUTION APPROACH

What is proposed is a Pilot Program to model the key industry sectors of the Critical Infrastructure in order to engage the teams in these industry sectors in a common cause of understanding the integration engineering steps needed to produce a harmonized Critical Infrastructure system of systems with particular attention to the identification of cascade triggers and an effective collaborative cross-sector way of working that will help sustain organization focus on this important issue.

Not just a problem diagnosis, the Pilot Program represents a bold step towards a problem solution. Based on an architecture of resilience, the Pilot Program would provide convincing evidence of the political will, technological leadership, innovative thinking, and public/private collaboration needed to meet one of the most consequential challenges of Cyber Security facing the nation and would do so on a milestone schedule, shown below, established by the Cyber Commission's period of performance scheduled to conclude on December 1, 2016.

The Pilot Program represents the first increment of a Critical Infrastructure model of operational resilience, one that emphasizes data flow, interfaces, state transitions, and interactions among industry sectors systematically recorded as nodes and arcs annotated with inputs and frequencies in the form shown below. As an artifact of infrastructure itself, the model is intended to be refined and extended to reflect an emerging understanding of the operational complexities among industry sectors, potential cascade triggers are anticipated and identified, intelligent distributed supervisory control tactics are formulated to avoid their effects, and the need and opportunity for additional digital situation awareness to support anticipation becomes more clear. The result sought is an operationally resilient Critical Infrastructure model that will guide the integration engineering of industry sector systems into the Situation System, Respondent System, and System Assets of the system of systems architecture, all described in my paper submitted to the Cyber Commission entitled, "*Integration Engineering in the Pursuit of Critical Infrastructure Resilience: The Role of the Resilience Integrator".*

PILOT PROGRAM RESEARCH VISION

Can a Cyber Security Perfect Storm be triggered by a single fast moving attack? Or does it take a carefully coordinated attack scenario? In any event, what tactics offer the best protection? More specifically, what is the least set of supervisory control operations best able to sustain a system of harmoniously cooperating distributed processes? To what extent is this set of operations currently embedded in the nation's critical infrastructure? What improvements are indicated to elevate that protection to a minimally acceptable state?

The Pilot Program would serve as a visible demonstration of software innovation and would provide a roadmap and tool for renovating the risk management paradigm employed for similar complex problems. The initial steps would be aimed at bounding the problem for research while preserving and building-in the scalability of the research models envisioned.

Goal

- Obtain intellectual control of targeted properties of the nation's critical infrastructure through supervisory control policies and protocols.

Objectives

- Model the supervisory control policies and protocols of selected sectors within the critical infrastructure along with their interactions and the behavior of targeted properties.
- Determine the predictive impacts related to the behavior of targeted properties while operating under various levels of stress.
- Assess the effectiveness of selective prescriptive measures introduced through changes in supervisory control policies and protocols in alleviating levels of stress.

REHABILITATING GOVERNMENT REPUTATION FOR CYBER SECURITY

Such a program would be a much needed step in rehabilitating the Government reputation for Cyber Security.

4. One Cyber Commission member stated that the government is considered a laughing stock in Cyber Security.
5. Another observed that there was animosity towards Government in Silicon Valley.

6. Still another observed that the government cannot do this by itself.
7. Echoing a similar note, a member observed that the topics are too much for the Cyber Commission.
8. Another lamented that there are no measurements.
9. Finally one member asked, *"What was the least amount of information that can be collected that everyone could agree to?"*

Where are the Jasons when we need them? If the Cyber Commission is to be the tip of the spear in the battle for Cyber Security, it appears that its work is cut out in preparing for such an engagement. Yet we are still left with two questions at the outset:

4. "*Are the Cyber Commission members selected adequate to the task as scoped by the President's Executive Order?"*
5. *Do the chosen topics for Cyber Commission deliberation adequately frame the Cyber Security challenge the nation faces?*

A bibliography might help members of the Cyber Commission to begin to evolve a shared culture. The start of such a bibliography has been attempted and attached below.

CYBERSPACE: STRATEGIC ADVANTAGE OR DISADVANTAGE

If Cyberspace, once a strategic advantage, is at risk of becoming a strategic disadvantage, there is a genuine need to show results on a hard problem. Today it is clear that more than public/private partnerships and soft change management approaches are needed to solve what is essentially an integration engineering problem with broad scope and deep complexity and an environment of independent silos of diverse domain engineering knowledge and approaches; systems and software engineering practices; and diverse industry sector business value propositions spanning trust, loyalty, and satisfaction. Instead what is needed is a Critical Infrastructure Resilience Manhattan Project with strong technical underpinnings coupled with equally strong technological and experienced leadership. The individuals expected to populate the industry sector teams are engineers who always find themselves struggling with an unsolved equation not lawyers and business MBA's skilled in rules, process, and governance.

A SENSE OF URGENCY

More than anything, the Critical Infrastructure Resilience Pilot Program needs to begin so that it can generate the momentum needed to sustain itself through the transition of Administrations. Getting a full head of steam while the Cyber Commission is still seated is the best bet. Starting this program, and starting it now, in itself would represent a visible demonstration of political will and leadership.

It would appear that the NIST Cyber Security Center of Excellence (NCCoE) is a natural point of responsibility to facilitate an immediate go ahead for this critical initiative.The (NCCoE) has an exceptional industry outreach infrastructure and exceptional engineering capabilities. Coupled with the necessary experienced technical management, this combination would posses the capability of the Resilience Integrator needed to address monthly milestone schedule attached.

I hope that each of you and the Cyber Commission members will find my comments, approach, and critique useful in coping with the Cyber Security challenges we all face.

Best Regards

Don O'Neill
Independent Consultant
ONeillDon@aol.com

Former President (2005-2008)
Center for National Software
Studies

Resources Previously Provided to the Cyber Commission

1. IBM Research Resource Report (draft): *Integration Engineering in the Pursuit of Critical Infrastructure Resilience: The Role of the Resilience Integrator*
2. Comments Delivered to the Commission onEnhancing National Cyber Security at the Kickoff Meeting on April 14, 2016
3. Letter to Chair and Vice Chair, Commission on Enhancing National Cyber Security, Subject: Cyber Commission Kickoff Followup: A Demonstration of Political Will and Technological Leadership to Protect Our Cyberspace Strategic Advantage, April 17, 2016

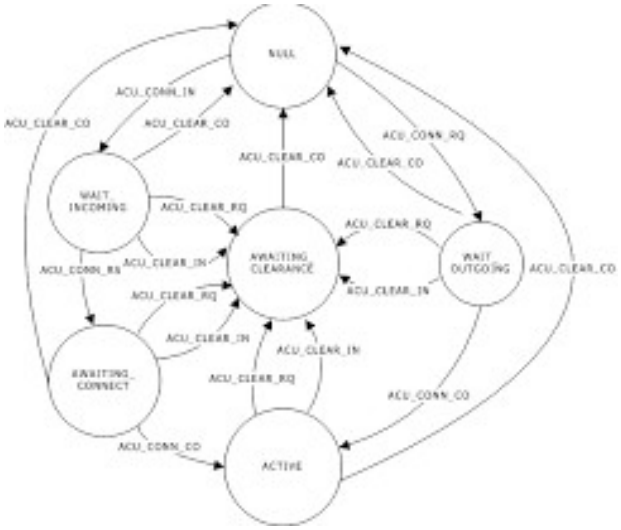
Bibliography

- Mead, N., Woody, C. (2016) "*Cyber Security Engineering: A Foundation of Operational Security",* Software Engineering Institute Carnegie Mellon University, SEI Series in Software Engineering, ISBN 978-0134189802, August 2016
- Jacobson, I., Lawson, H.B. (2015) "*Software Engineering in the Systems Context"*, Edited by Ivar Jacobson and Harold "Bud" Lawson, College Publications, Kings College, London, ISBN 978-1-84890-76-6, 2015, 578 pages
- Koppel, T. (2015), "*Lights Out",* Crown Publishing Group, 2015, ISBN 978-0-553-41996-2, 277 pages
- Lewis, Michael (2014) "*Flash Boys: A wall Street Revolt",* W.W. Norton and Company, Ltd., ISBN 978-0-393-24466-3, 2014, 274 pages
- Herman, Arthur (2012), *"Freedom's Forge: How American Business Produced Victory in World War II",* The Random House Publishing Group, 2012, ISBN 978-1-4000-6964-4, 413 pages
- Clarke, Richard A., Knake, R, B, (2010) *"Cyber War: The Next Threat to National Security and What to Do About It",* Harper-Collins Publishers, 2010, ISBN 978-0-06-196223-3, 290 pages
- Kramer, F. D., Starr, S. H., Wentz, L. K. (2009), "*Cyberpower and National Security",* National Defense University ,Potomac Books, Inc., ISBN 978-1-59797-423-3, 2009, 642 pages
- Finkbeiner, Ann (2007), "*The Jasons: The Secret History of Science's Postwar Elite",* Penguin Books, 2007, ISBN 978-0-14-303847-4, 304 pages

Convincing Evidence of the Presence of Political Will
To Pursue a Resilient Critical Infrastructure System of Systems

Milestone Schedule	Pilot Program Tasks
April 2016	Select Critical Infrastructure industry sectors to pilot and identify named representative for each industry sector
May 2016	Obtain shared vision on the value proposition and integration engineering approach and produce an operational concept of industry sector interactions and state transitions.
June 2016	Model the system of systems architecture selected, demonstrate the model, and exercise it with an eye on industry sector interfaces, state transitions, and cascade trigger identification and mitigation.
July 2016	Select the team in each industry sector to collaborate and implement the Situation System.
July 2016	Select the team to collaborate and implement the Respondent System behavior associated with digital situation awareness and distributed supervisory control
July 2016	Select the team to collaborate and implement System Assets needed for defense in depth, business process continuity, and survivability.
August 2016	Obtain shared vision among the teams on the way of working based on principles and foundations established.
August 2016	Initiate the work.
September 2016	Identify work products to be produced and inspected for completeness, correctness, consistency, and achievement of value add.
October 2016	Assess resilience assurance of the Critical Infrastructure using the resiliency risk and earned value calculation spreadsheet and worksheet.
November 2016	Pilot Program Initial Operating Capability needed to model the effectiveness of shutdown, minimum essential function, coordinated recovery time objectives, and cascade triggers.
December 2016	Pilot Program increment concluded.

State Machine expressed as nodes and annotated arcs



2196 words