The just released White House Cyber Security National Action Plan (CNAP) contains a provision entitled, "Enhance Critical Infrastructure Security and Resilience". Treatment of Critical Infrastructure Resilience in the context of the CNAP provision is illustrated in the following YouTube. The material for this YouTube presentation is drawn from the recently published book entitled, "Software Engineering in the Systems Context", and Chapter 4 "Applying a Systems Perspective in Addressing Critical Infrastructure Resilience" which I authored along with several other chapters.

Subject: User Story: Critical Infrastructure Resilience
http://youtu.be/1Ksw6HwO5SY

25:51 minutes

Description:
The critical infrastructure is the industrial base on which the competitiveness and security of a nation are dependent. The current state of a nation's critical infrastructure is at risk. The Internet has become the central nervous system of a nation both private and public. A nation's critical infrastructure continues to be vulnerable to natural disasters and cascading Cyber Security attacks.

Accordingly and within the context of the YouTube presentation, an update to the Cyber Framework is suggested in accordance with CNAP .
1. The role of a Critical Infrastructure Resilience Integrator needs to be specified as follows:
a. Conduct industry sector assessments of the Resiliency Maturity Framework and pinpoint the gaps at each level.
b. Conduct industry sector assessments of the shortfall in context and culture challenges.
c. Conduct industry sector assessments of unresolved Technical Debt spanning management, process, and engineering.
d. Conduct industry sector assessments of readiness to fulfill the Intelligent Middleman job description.
e. Specify the requirements and program plan for engineering, developing, and fielding the Critical Infrastructure Resilience Systems of Systems Architecture of the Respondent System in accordance with the specified architecture rules of construction.

Don O'Neill
Independent Consultant

CNAP
Enhance Critical Infrastructure Security and Resilience The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure. A continued partnership with the owners and operators of critical infrastructure will improve cybersecurity and enhance the Nation's resiliency. This work builds off the President's previous cybersecurity focused Executive Orders on Critical Infrastructure (2013) and Information Sharing (2015).

- 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 Cybersecurity 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.
- The Department of Homeland Security will double the number of cybersecurity advisors available to assist private sector organizations with in-person, customized cybersecurity assessments and implementation of best practices.
- The Department of Homeland Security is collaborating with UL and other industry partners to develop a Cybersecurity Assurance Program to test and certify networked devices within the "Internet of Things," whether they be refrigerators or medical infusion pumps, so that when you buy a new product, you can be sure that it has been certified to meet security standards.
- The National Institute of Standards and Technology is soliciting feedback in order to inform further development of its Cybersecurity Framework for improving critical infrastructure cybersecurity. This follows two years of adoption by organizations across the country and around the world.
- Yesterday, Commerce Secretary Pritzker cut the ribbon on the new National Cybersecurity Center of Excellence, a public-private research and development partnership that will allow industry and government to work together to develop and deploy technical solutions for high-priority cybersecurity challenges and share those findings for the benefit of the broader community.
- The Administration is calling on major health insurers and healthcare stakeholders to help them take new and significant steps to enhance their data stewardship practices and ensure that consumers can trust that their sensitive health data will be safe, secure, and available to guide clinical decision-making.