MITRE

Cyber Resiliency FAQ

This FAQ document fosters knowledge by providing commonality in cyber resiliency terms and concepts. Cyber resiliency supports mission assurance goals for systems and systems-of-systems (SoS). Because of increased threats and their wide-reaching implications, progress and innovation in the field first require a common understanding of terminology and concepts. The answers to these FAQs establish a bedrock of understanding for professionals on an increasingly complex topic.

1. What is cyber resiliency?

Cyber resiliency (also referred to as cyber resilience) is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.1

2. What is the source for this definition of cyber resiliency?

There is no single authoritative definition for cyber resiliency. The definition provided above is drawn from definitions of resilience and resiliency used by different communities of interest as shown in the table below.

Context	Term	Definition
National Security	Resilience	"The ability to ***adapt*** to changing conditions and ***prepare*** for, ***withstand,*** and rapidly ***recover*** from disruption." [WH 2010]
Critical Infrastructure	Infrastructure resilience	"Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to ***anticipate, absorb, adapt*** to, and/or rapidly ***recover*** from a potentially disruptive event." [NIAC 2010]
Critical Infrastructure Security and Resilience	Resilience	"…the ability to ***prepare*** for and ***adapt*** to changing conditions and ***withstand*** and ***recover*** rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." [WH 2013]
DoD Cybersecurity	Operational resilience	"The ability of systems to ***resist, absorb,*** and ***recover*** from or ***adapt*** to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions." [DoD 2014]

[1] It is outside the scope of this FAQ to define "cyber" or "resilience" in general. However, because the definition of "cyber resiliency" includes the term "cyber resources," that term must be defined. Cyber resources are defined as "separately manageable resources in cyberspace, including information in electronic form, as well as information systems, systems-of-systems, network infrastructures, shared services, and devices" (derived from NIST SP 800-39 [NIST 80039]). "Cyberspace" is defined as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Derived from [CNSS 4009], cited in [NIST 80039]).

Network Engineering	Resilience	"The ability of the network to provide and ***maintain*** an acceptable level of service in the face of various faults and challenges to normal operation." [Sterbenz 2006]
Resilience Engineering	Resilience engineering	"The ability to build systems that are able to ***anticipate*** and circumvent accidents, survive disruptions through appropriate learning and ***adaptation,*** and ***recover*** from disruptions by restoring the pre-disruption state as closely as possible." [Madni 2009]
Homeland Security	Resilience	The ability to ***adapt*** to changing conditions and ***prepare*** for, ***withstand,*** and ***rapidly*** recover from disruption." [Risk 2010]

These definitions have various commonalities. Each expresses:

- A common theme of addressing situations or conditions in which disruption, adversity, errors, faults, or failures occur [Solutions, 2017].
- Consistent resiliency goals (shown in bold italics above) when encountering situations or conditions causing disruption, adversity, and faults: recover, withstand (i.e., maintain or resist), adapt (i.e., evolve), and anticipate (i.e., prepare).

Thus, the cyber resiliency definition of "**the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources**" is consistent with the above themes and goals.

3. Why is cyber resiliency needed?

Cyber resiliency is needed to sustain capabilities provided by cyber resources despite the activities of threat actors that can penetrate and achieve a presence within a targeted organization's cyber infrastructure.

The sources of attacks or compromises considered by cyber resiliency specifically include the advanced persistent threat (APT).[2] The APT is far more sophisticated and capable than more conventional threat actors, such as individual criminals, hackers, or privilege-abusing insiders. The APT cannot always be kept out of a system or be quickly detected and removed from that system, regardless of the quality of the system design, the functional effectiveness of the security components, and the trustworthiness of the selected components. The need for cyber resiliency was well summed up by Lt. Gen. Ted F. Bowlds, former Commander, Electronic Systems Center, USAF:

> *"You are going to be attacked; your computers are going to be attacked, and the question is, how do you fight through the attack? How do you maintain your operations?" [Hanscom 09]*

[2] The Joint Task Force Transformation Initiative (DoD, ODNI, and NIST) defines the APT as: an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. [NIST 80053] The term "advanced cyber threats" is used in [DSB 2013] and the term "malicious cyber activity" is used in [DoD 2015].

4. To what does cyber resiliency apply?

Cyber resiliency can apply to a system, a system-of-systems, a mission, a business function, an organization, or a cross-organizational mission. The cyber resources, and the range of adversity to which cyber resources are susceptible, vary depending on the context in which "cyber resiliency" is sought. In any situation, the underlying assumption is that the mission or business function to be made cyber resilient depends on cyber resources to do something, and that "adverse conditions, stresses, attacks, or compromises" create risk due to that dependence.

5. Why address cyber resiliency in the acquisition process?

Incorporating cyber resiliency measures into the acquisition process increases the likelihood that the system will continue to provide mission-critical and mission-essential capabilities in spite of adversarial actions, and will give cyber defenders the necessary tools to respond quickly and effectively to the adversary. Moreover, if the resiliency measures incorporated into the acquisition are sufficiently flexible and extensible, they will increase cyber defenders' ability to adapt to and parry adversary actions. Such cyber resiliency capabilities as deception nets, defense-in-depth architectures, and the use of heterogeneous applications, operating systems, and platforms cannot readily be added to an existing system, but must be designed into the system early.

In the case of the DoD acquisition process, incorporating cyber resiliency is consistent with the DoD Cyber Strategy [DoD 2015b]. It states, "Because the Defense Department's capabilities cannot necessarily guarantee that every cyberattack will be denied successfully, the Defense Department must invest in resilient and redundant systems so that it may continue its operations in the face of disruptive or destructive cyberattacks on DoD networks." DoD and the General Services Administration (GSA) have developed recommendations for improving cybersecurity and resilience through acquisition [DoD 2013].

6. How does cyber resiliency relate to existing acquisition guidance?

The JCIDS Manual [DoD 2015a] Appendix A, Enclosure D, defines the System Survivability Key Performance Parameter (KPP). The Joint Capabilities Integration and Development System (JCIDS) Manual [DoD 2015a], Appendix C, states "Include whether or not the system must be able to survive and operate in a cyber-contested environment or after exposure to cyber threats which prevent the completion of critical operational missions by destruction, corruption, denial, or exposure of information transmitted, processed, or stored." The DoD Instruction on Cyber Security [DoD 2014] establishes general requirements for operational resilience. The DoD Cybersecurity Test and Evaluation Guidebook [DoD 2015c] supports the goal of operational resilience defined by DoDI 8500.01; one question to be answered by testing is, "How resilient is the system to cyber-attack when supporting mission operations?"

7. How does cyber resiliency relate to mission assurance and mission continuity?

Cyber resiliency enables or supports mission/business assurance and mission/business continuity by focusing on the cyber resources on which a mission depends. It aims to maximize an organization's ability to complete critical mission functions despite an adversary presence in the organization infrastructure. Cyber resiliency enables an organization to "fight through" even when an adversary has achieved a persistent foothold in the organization's cyber infrastructure.

8. What types of threats does cyber resiliency address?

Cyber resiliency *focuses* on addressing the APT [NIST 80039], but it *addresses* all threats to cyber resources, whether such threats are cyber or non-cyber (e.g., kinetic) in nature.

The resources associated with the APT, its stealthy nature, its persistent focus on the target of interest, and its ability to evolve in the face of defender actions make it a highly dangerous threat. Moreover, APT actors can take advantage of or make their behavior appear to result from other forms of adversity, including human error, structural failure, or natural disaster. Thus, focusing on potential effects of APT activities enables defenders to anticipate, withstand, recover from, and adapt to a broad suite of adverse conditions and stresses on cyber resources. This maximizes mission continuity despite the presence of an adversary in a system, including an adversary that may be masquerading as other representative adverse events such as software and operator errors, failures of supporting infrastructures (e.g., power), and natural events with cyber effects (e.g., solar weather that affects satellite communications).

9. Is cyber resiliency simply another name for cybersecurity?

No, cyber resiliency differs from cybersecurity[3] as conventionally employed in two ways:

- Cybersecurity focuses on achieving the security objectives of confidentiality, integrity, and availability to acceptable levels, conventionally by using a combination of perimeter protections and internal controls such as identity and access management (IdAM) and intrusion detection and response (IDR). In contrast, the goals of cyber *resiliency – anticipate, withstand, recover, and evolve* – are derived from the discipline of resilience engineering. Cyber resiliency does complement cybersecurity objectives. The cyber resiliency goals are particularly relevant as applied to missions in the context of their dependency on cyber resources. Cyber resiliency links mission assurance and cybersecurity, overlapping with each in some ways and yet distinct from each in other ways, moving beyond (while complementing) the "Identify, Protect, Detect, Respond, and Recover" model [NIST 2014].

- The threat model, and risk-framing decisions, for cybersecurity, as conventionally employed, (e.g., as expressed in the NIST SP 800-53R4 baselines, or in Tiers 1 - 3 of the NIST Cybersecurity Framework [NIST 2014]) assumes that the adversary can be kept out of a system or can be quickly detected and removed from that system. In contrast, cyber resiliency is based on the assumption that a sophisticated adversary can overcome such conventional measures as boundary protections, IdAM, IDR, and continuity of operations (COOP) measures. The threat model for cyber resiliency takes into consideration supply chain contamination, long adversary

[3] "The US Federal Government defines generally accepted standards of good cybersecurity practice in FIPS 199 [FIPS 199] and the baselines defined in NIST SP 800-53R4 [NIST 80053]. As identified in the NIST SP 800-53R4 baselines [NIST80053] and the NIST Cybersecurity Framework (through Tier 3) [NIST 2014], these currently focus on boundary protection, identity and access management, intrusion detection and response (or intrusion prevention and response), and continuity of operations (COOP). The series of publications by the Joint Transformation Initiative (JTI) – including NIST SP 800-39 [NIST 80039], NIST SP 800-53R4 [NIST 80053], and NIST SP 800-30R1 [NIST 80030] – include consideration of advanced cyber threats [DSB 2013] and cyber resiliency. However, organizations using those publications can restrict themselves to non-APT threats based on their risk framing. (In Task 1-1 (Risk Assumptions) of Risk Framing in [NIST 80039], the organization identifies its assumptions about the threats it faces.)

dwell times, and loss of control over parts of the set of cyber resources on which an organization depends.

10. Is cyber resiliency a replacement for cybersecurity?

No, cyber resiliency works in conjunction with cybersecurity. Most cyber resiliency measures assume, leverage, or enhance a variety of cybersecurity measures. Cybersecurity and cyber resiliency measures are most effective when applied together in a balanced way. The cyber resiliency perspective reflects that modern systems are large and complex entities, and as such systems, operational environments, and supply chains will always have flaws and weaknesses that adversaries will be able to exploit. Given resource limitations, achieving sufficiently effective defense of systems and missions requires making trade-offs among measures to achieve cybersecurity objectives and cyber resiliency objectives.

11. How does cyber resiliency apply in the cyber attack life cycle/cyber kill chain?

Cyber resiliency measures (i.e., architectural decisions, technologies, operational practices) are predicated on the assumptions that an adversary can achieve a foothold in an organization's systems, and that post-exploit adversary activities must be thwarted. However, most cyber resiliency measures have effects on adversary activities across the cyber attack life cycle.

12. What is the relationship between cyber resiliency and concepts such as disaster recovery, business continuity, and COOP?

Cyber resiliency shares with those disciplines the goals of continuity (withstanding adversity) and recovery. It differs in its underlying threat model however, and thus in the techniques that can address adversity. The other disciplines, developed over many decades, often assumed one-time threat events, non-guided attacks, and threat events that are generally physical in nature. While cyber resiliency addresses all those types of threat events as directed at cyber resources, it also deals with cyber-based threat events, for which physical and geographic separation of duplicate resources (a common mitigation technique for non-cyber sourced threat events) is not an effective mitigation. In addition, cyber resiliency does not assume a one-time event or a period of quiescence after an event; its threat model recognizes that, due to the stealthy and persistent nature of the APT, reconstitution may have to occur while attacks continue. Cyber resiliency requires recognition that the defender is dealing with an aware and intelligent adversary and that the adversary may actually be evolving and adapting its actions in response to the defender's actions. Thus, systems and cyber defenders seek as feasible to change their behavior on an ongoing or frequent basis, rather than implement relatively static plans and playbooks.

13. Don't the NIST and CNSSI baselines provide for cyber resiliency?

The NIST and CNSSI baselines partially and incidentally identify cyber resiliency controls.

NIST Special Publication 800-53 explicitly states that it does not consider the APT as one of the assumptions underlying the baselines. The inclusion of any security controls in those baselines that focus on resiliency is largely incidental.

CNSSI 1253 baselines do include the APT in their assumptions. Of the approximately 150 cyber resiliency controls included in NIST SP 800-53 [Bodeau 2013], only about 60 are included in the CNSSI 1253 High-High-High (HHH) baselines (and a lower number and percentage in the other baselines). In other words,

approximately 13% of the HHH baseline's 460+ controls focus on resiliency. The selected HHH resiliency controls focus largely on enhancing aspects of cybersecurity (e.g., detecting the adversary, analyzing its actions, and recovering from those actions); those are important, but do not address all aspects of cyber resiliency.

NIST SP 800-53 mentions cyber resiliency controls that focus more on disrupting the attack surface, thereby impeding the adversary's ability to obtain correct and timely information about defensive capabilities, and cause the adversary to make incorrect assumptions about the system or its defensive capabilities, waste resources, or prematurely disclose malware to cyber defenders. These controls are not selected in any baseline.

14. How does cyber resiliency relate to the Risk Management Framework (RMF)?

The RMF and cyber resiliency are compatible concepts. This holds true whether the RMF is considered an organizational approach to risk management (frame, assess, respond, and monitor); an application of that approach at the mission / business process tier to define enterprise, mission segment, and information security architecture; or a set of steps that apply the approach to an information system (using the six steps in NIST SP 800-37 and DoDI 8500.01). For an information system, cyber resiliency fits particularly well into the RMF step for selecting and tailoring NIST SP 800-53 controls and associated baselines. The process of tailoring such baselines to add resiliency-specific controls and potentially trade off conventional security-focused controls for cyber resiliency-focused controls is totally consistent with the RMF. From the RMF perspective, regardless of whether one is looking at the organization, mission, or system level, the relative concern for cyber resiliency, and how to handle the threat posed by the APT, is simply one specific factor to consider in making risk management trade-offs.

15. How does cyber resiliency relate to system security engineering?

Systems security engineering (SSE) is a specialty discipline of systems engineering, focused on the protection of stakeholder and system assets so as to exercise control over asset loss and the associated consequences [NIST 800160]. Proper implementation of SSE takes cyber resiliency into consideration by treating mission capabilities as stakeholder assets and by addressing consequences to current and future missions.

Cyber resiliency can be addressed throughout the SSE technical processes [Ross et al., 2016][4]. Cyber resiliency is addressed across the processes as follows:

- The cyber resiliency goals provide a useful context for eliciting operational concepts during the *Security Concepts Definition* within SSE.
- Cyber resiliency approaches can be incorporated into *Security Design* (taking into consideration interdependencies and potential interactions [Bodeau 2015]).
- The cyber resiliency objectives provide a context for eliciting stakeholder protection imperatives within the *Protection Needs Definition* process.

Cyber resiliency is more specifically addressed in four of the technical processes shown in the figure above:

- Cyber resiliency requirements (and corresponding cyber resiliency controls [Bodeau 2013]) can be identified as part of *Security Requirements Definition*.

[4] These are based on standard systems engineering technical processes [ISO 2015].

- Cyber resiliency design principles can be defined and applied as part of the *Secure Architecture Design* process.
- Cyber resiliency will be tested as part of *Security Verification* and *Security Validation* processes [DoD 2015c].
- Operational improvements to cyber resiliency can be made as part of the *Secure Operations* process.
- Changes to technical capabilities that improve cyber resiliency can introduced as part of the *Secure Maintenance* process.

16. Is there an optimum set of cyber resiliency measures?

No single set of cyber resiliency measures (architectural decisions, technologies, operational practices) is appropriate across all environments and systems. Various factors must be considered in the selection process. These include:

- Political, operational, economic, and technical factors
- Relative maturity and adoption of the measures
- Time frame (e.g., incorporating resiliency into a new acquisition or updating a relatively mature system)
- Environment (e.g., command and control system, SoS, critical infrastructure systems, embedded systems).

Mission and operations managers, and program managers, need to consider all these factors, along with the priorities, concerns, and risk tolerance of the various stakeholders in selecting the optimum set of resiliency measures.

17. Isn't cyber resiliency simply concerned with returning to normal operating conditions in a specified time period?

Cyber resiliency focuses on maximizing mission assurance. This question limits cyber resiliency to the goal of a defined recovery. Recovery – returning to a known good state in some defined time period after a cyber event occurs – is one desired outcome of cyber resiliency. However, it may not always be feasible; some adversary activities can make the state of a system indeterminate, while other adversary activities can be sufficiently destructive that an acceptable level of service cannot be restored. It may be useful to view a system's being resilient to a cyber attack as similar to an individual's being resilient to cancer: a cure may not be feasible, especially after the cancer metastasizes. Instead, resilience focuses on maximizing the patient's life span and quality of life. Likewise, cyber resilience focuses on maximizing the mission/business assurance despite the presence of adversary activities.

18. How much cyber resiliency is enough? How is cyber resiliency evaluated?

- No single correct answer exists. "How much" is a risk management decision, while "how to evaluate" (using cyber resiliency metrics or assessment methods) depends on the evaluation environment and on the context in which the question is asked (e.g., a mission context, a controls effectiveness context, or an architectural context).
- The evaluation environment can be operational, limited (e.g., a cyber range, a test and evaluation enclave), or purely analytic. To ensure realism, evaluation (particularly in a mission or controls context) typically relies on retrospective analysis of events in an operational environment or on emulation (e.g., via a Red Team) in a limited environment. However,

assessment in a purely analytic environment, while less realistic, can consider a wider range of possible attacks and can be used in all contexts.

- In any context, evaluation of "how much" or "how effective" is predicated on assumptions about adversary characteristics. Because advanced cyber adversaries adapt their tactics, techniques, and procedures (TTPs), assessments of cyber resiliency are inherently more uncertain than assessments of other capabilities (e.g., reliability, maintainability).
- In a mission context, "how much" relates to how quickly, how completely, and with how much confidence mission functions can be restored or mission capabilities can be reconstituted. It may also relate to how well mission-critical functions can be performed while a cyber attack is ongoing. Thus, cyber resiliency assessment can be part of assessing mission Measures of Effectiveness (MOEs), Measures of Performance (MOPs), and KPPs.
- In a context of controls effectiveness, "how much" relates to effects on adversary activities. For example, the length of time an adversary continues to operate in a deception environment is a measure of the effectiveness of deception measures. The length of time between compromise of resources in one enclave or segment and compromise of similar resources in another enclave is a measure of the effectiveness of segmentation.
- In an architectural context, "how much" relates to achieving cyber resiliency objectives, applying cyber resiliency design principles, or integrating cyber resiliency techniques into the architecture. Assessment in this context is more likely to be qualitative or semi-quantitative, and can be part of evaluation of Key System Attributes (KSAs).

19. Is cyber resiliency the same as fault tolerance?

While these two concepts are related, they are not the same. Fault tolerance is the extent to which a functional unit will continue to operate at a defined performance level even though one or more of its components are malfunctioning [Solutions, 2017]. Cyber resiliency is related, but different. It is the ability to **anticipate, withstand, recover** from, and **adapt** to adverse conditions, stresses, attacks on, or compromises of cyber resources.

Both fault tolerance and cyber resiliency are concerned with continuing operations. A major difference, however, is the focus of each discipline. Fault tolerance focuses on faults or failures, which are commonly results of human errors, or of stresses or operating conditions near the boundaries of the set of conditions as defined or assumed in the system specification. Cyber resiliency focuses on *adversarial threats* – but, because adversaries can emulate or leverage other forms of adversity or stress, it may also consider faults, failures, human errors, natural disasters, and failures of supporting infrastructures. As a result, fault tolerance usually does not assume ongoing, stealthy, evolving threat-actors or agents, and is not concerned with adapting/evolving in response to a successful threat event. Finally, cyber resiliency comes into play when cyber components are part of a system or SoS. Fault tolerance applies to systems that may include cyber components as well as to those that do not.

20. Where can I find more information on cyber resiliency?

More information about cyber resiliency is available on the right-hand panel of www.mitre.org/cyberworkshop**.** For additional information please contact secureandresilient@mitre.org

References

[Bodeau 2013] Bodeau, D, and Graubart, R., "Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls" (MTR 130531, PR 13-4037), September 2013. http://www.mitre.org/sites/default/files/publications/13-4047.pdf

[Bodeau 2015] D. Bodeau, R. Graubart, W. Heinbockel and E. Laderman, "Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques" (MTR140499R1, PR 15-1334), May 2015. http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf.

[CNSSI 1253] Committee on National Security Systems (CNSS) Instruction 1253, Version 2, *Security Categorization and Control Selection for National Security Systems*, March 2014.

[CNSS 4009] Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance (IA) Glossary*, April 2015.

[DoD 2013] Department of Defense (DoD) and General Services Administration (GSA), "Improving Cybersecurity and Resilience through Acquisition: Final Report of the Department of Defense and General Services Administration," in *(transmittal memorandum dated 23 January 2014)*, 2013. http://www.gsa.gov/portal/mediaId/185367/fileName/IMPROVING_CYBERSECURITY_AND_RESILIENCE_THROUGH_ACQUISITION.action

[DoD 2014] DoDI 8500.01, Cyber Security, March 14, 2014. http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

[DoD 2015a] "Manual for the Operation of The Joint Capabilities Integration and Development System (JCIDS)," 12 February 2015. https://dap.dau.mil/policy/Documents/2015/JCIDS_Manual_-_Release_version_20150212.pdf

[DoD 2015b] "The Department of Defense Cyber Strategy," April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[DoD 2015c] "Department of Defense Cybersecurity Test and Evaluation Guidebook, Version 1.0," 1 July 2015. http://www.dote.osd.mil/docs/TempGuide3/Cybersecurity_TE_Guidebook_July1_2015_v1_0.pdf

[DSB 2013] Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[FIPS 199] National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[Hanscom 2009] Hanscom Air Force Base, "General Bowlds delivers second State of ESC Address," 30 January 2009. http://www.hanscom.af.mil/news/story.asp?id=123133327.

[ISO 2015] International Standards Organization, International Standard ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*, 15 May 2015.

[Madni 2009] Madni, Azad M. and Jackson, Scott, "Towards a Conceptual Framework for Resilience Engineering." *IEEE Systems Journal, Vol. 3, No. 2,* June 2009.

[NIAC 2010] National Infrastructure Advisory Council (NIAC), *A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council*. October 19, 2010. http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf

[NIST 2014] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Security, Version 1.0," 12 February 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[NIST 80030] NIST Special Publication (SP) 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[NIST 80039] "NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[NIST 80053] "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[NIST 800160] "Systems Security Engineering: A Multidisciplinary Approach to Building Trustworthy Secure Systems (NIST SP 800-160 Second Public Draft)," forthcoming.

[Risk 2010] Risk Steering Committee, DHS Risk Lexicon, 2010 Edition. September 2010. http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

[Ross 2015] Ross, R., "NIST Special Publication 800-160, Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems (presentation)," 27 May 2015. http://www.isaca-washdc.org/presentations/2015/am2015_Day2Session4a.pdf

[Solutions 2017] Solutions, Alliance for Telecommunications Industry, *ATIS Telecom Glossary*. http://www.atis.org/glossary/annex.aspx

[Sterbenz 2010] Sterbenz, James P.G., et al., "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines" *Computer Networks* 54 (2010) 1245–1265. March 17, 2010.

[WH 2010] White House, National Security Strategy, May 2010. https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[WH 2013] PPD-21, Presidential Policy Directive-21, *Critical Infrastructure Security and Resilience,* February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil