



Building Cyber Resilient Systems

A National and Economic Security Imperative

Dr. Ron Ross
Computer Security Division
Information Technology Laboratory



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The Current Landscape.

It's a dangerous world in cyberspace...

Cyber Risk.

Function (threat, vulnerability, impact, likelihood)



Energy



Transportation

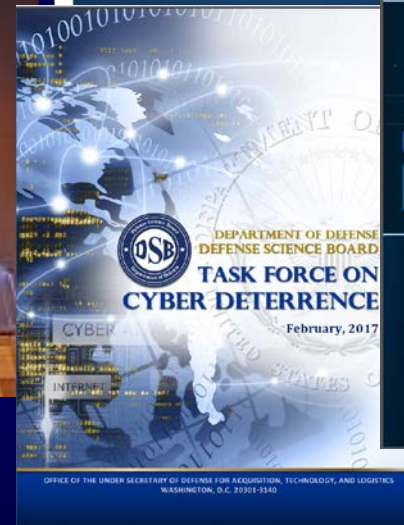
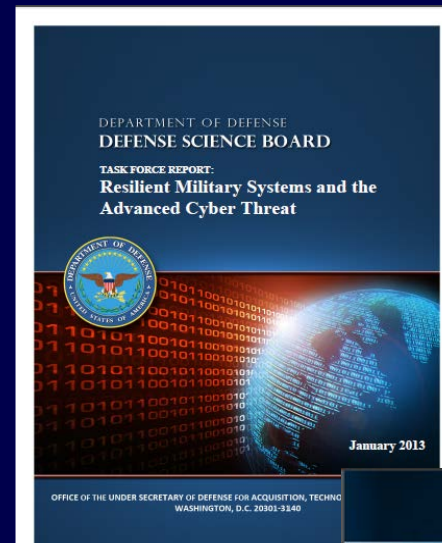


Manufacturing



Defense

- Resilient Military Systems and the Advanced Cyber Threat
 - Cyber Supply Chain
 - Cyber Deterrence



Defense Science Board Reports

Complexity.



Our appetite for *advanced technology* is rapidly exceeding our ability to protect it.



Data. Data. Everywhere.






Houston, we have a problem.

Protecting critical systems and assets and
making them cyber resilient—

*The highest priority for the national and economic
security interests of the United States.*





Defending cyberspace
in 2018 and beyond.



Reducing susceptibility to *cyber threats* requires a multidimensional strategy.

Harden the target

First Dimension



Limit damage to the target

Second Dimension

Make the target resilient

Third Dimension



- NIST SP 800-160, Volume 2

Systems Security Engineering

Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems



Cyber Resiliency.

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.



Distinguishing Characteristics

CYBER RESILIENCY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

FOCUS ON MISSION OR BUSINESS

Cyber resiliency focuses on capabilities supporting organizational missions or business functions. It maximizes the ability of organizations to complete critical or essential missions or business functions despite an adversary presence in their systems and infrastructure, threatening mission-critical systems and system components.



Distinguishing Characteristics

CYBER RESILIENCY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

FOCUS ON ADVANCED PERSISTENT THREAT

Cyber resiliency addresses threats to systems containing cyber resources, whether such threats are cyber or non-cyber (e.g., kinetic). But the focus of cyber resiliency is on the APT. The resources associated with the APT, its stealthy nature, its persistent focus on the target of interest, and its ability to adapt in the face of defender actions make it a highly dangerous threat.



Distinguishing Characteristics

CYBER RESILIENCY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

ASSUME ADVERSARY WILL COMPROMISE SYSTEM

A fundamental assumption of cyber resiliency is that a sophisticated adversary cannot always be kept out of a system or be quickly detected and removed from that system, despite the quality of the system design, functional effectiveness of the security components, and trustworthiness of the selected components.



Distinguishing Characteristics

CYBER RESILIENCY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

ASSUME ADVERSARY WILL MAINTAIN A PRESENCE

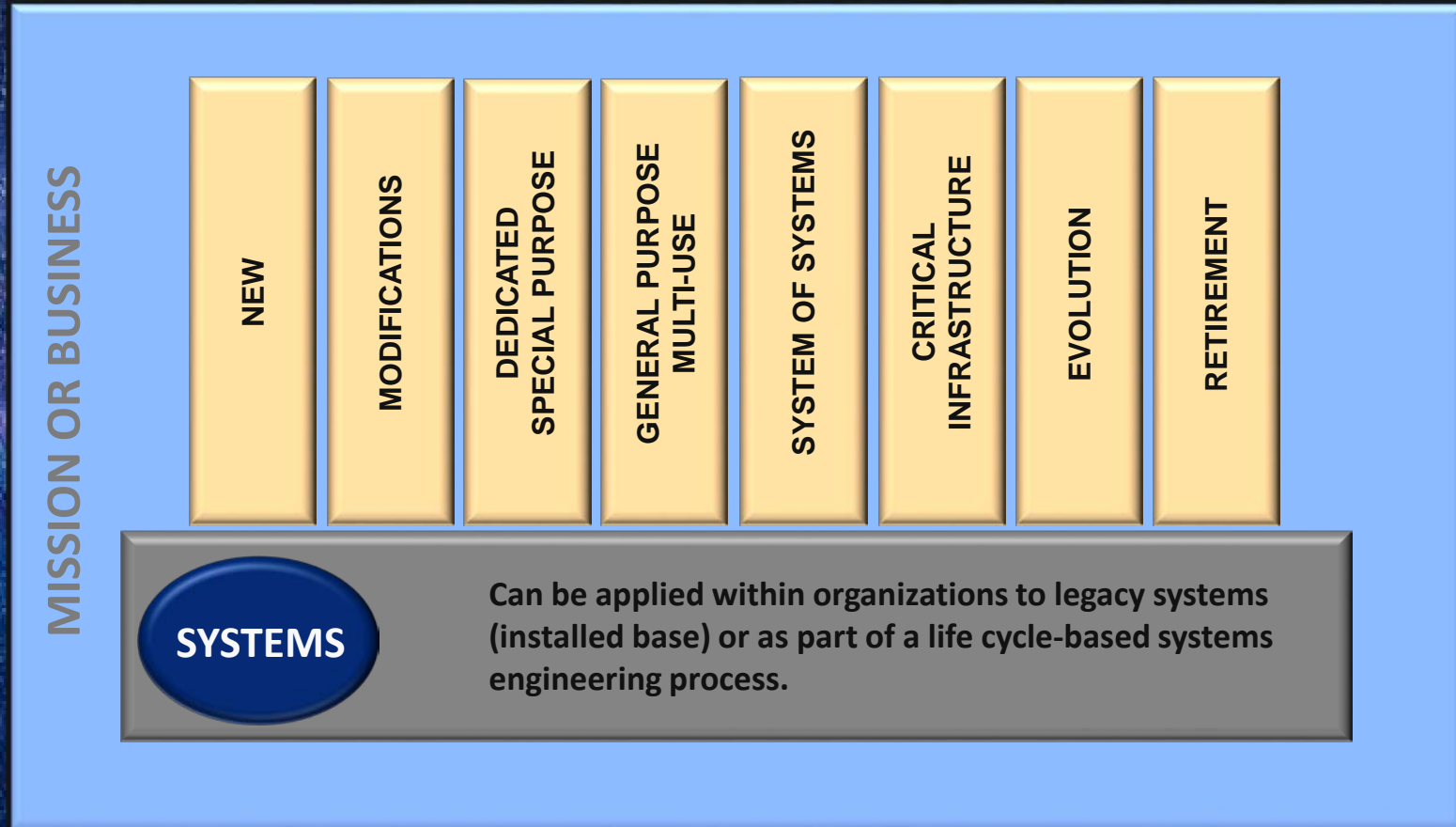
Cyber resiliency assumes that the adversary presence in the system may be a persistent and long-term issue—and recognizes that the stealthy nature of the APT makes it difficult for an organization to be certain that the threat has been eradicated. It also recognizes that the ability of the APT to adapt implies that mitigations that previously were successful may no longer be effective.



Cyber resiliency relationships with other specialty engineering disciplines.



Cyber Resiliency Applicability.





CREF

CYBER RESILIENCY ENGINEERING FRAMEWORK

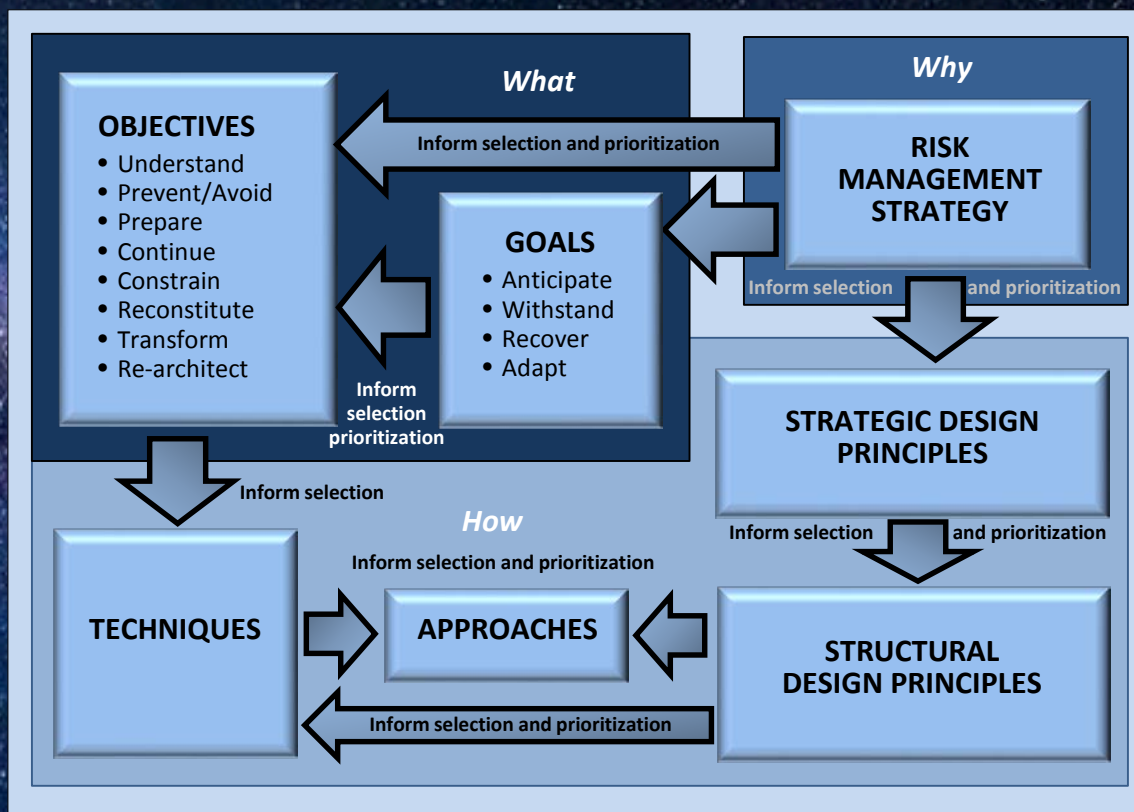
PROTECTION. DAMAGE LIMITATION. RESILIENCY.



Constructs

- Goals
 - Objectives
 - Techniques
 - Approaches
 - Strategic Design Principles
 - Structural Design Principles
 - Risk Management Strategy

Relationship among cyber resiliency constructs.





CREF

CYBER RESILIENCY ENGINEERING FRAMEWORK

PROTECTION. DAMAGE LIMITATION. RESILIENCY.



Objectives

- Prevent or Avoid
 - Prepare
 - Continue
 - Constrain
 - Reconstitute
 - Understand
 - Transform
 - Re-Architect



CREF

CYBER RESILIENCY ENGINEERING FRAMEWORK

PROTECTION. DAMAGE LIMITATION. RESILIENCY.



Techniques

- Adaptive Response
- Analytic Monitoring
- Coordinated Protection
- Substantiated Integrity
- Privilege Restriction
- Dynamic Positioning
- Dynamic Representation
- Non-Persistence
- Diversity
- Realignment
- Redundancy
- Segmentation
- Deception
- Unpredictability

Cyber Resiliency Constructs in System Life Cycle.



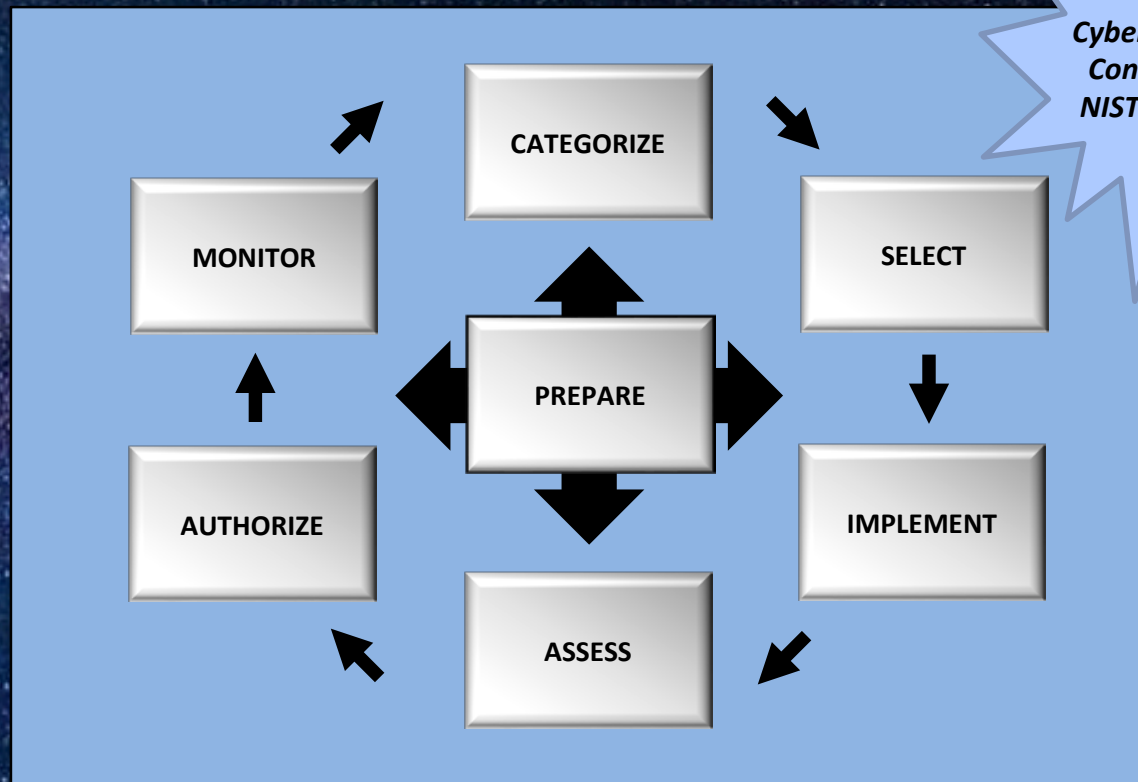
ISO/IEC/IEEE 15288:2015
Systems and software engineering
— *System life cycle processes*



- Business or mission analysis
- Stakeholder needs and requirements definition
 - System requirements definition
 - Architecture definition
 - Design definition
 - System analysis
 - Implementation
 - Integration
 - Verification
 - Transition
 - Validation
 - Operation
 - Maintenance
 - Disposal

NIST
SP 800-160

Cyber Resiliency and the Risk Management Framework.



*Cyber Resiliency
Controls from
NIST SP 800-53*

Some final thoughts.

Work smarter, not harder.



Transparency.

Traceability.

Trust.





Institutionalize.

Cyber Resiliency.



Operationalize.

Cyber resilient systems can not be achieved without planning and resources...



Leadership.
Governance.
Accountability.

On the Horizon...



- **NIST Special Publication 800-160, Volume 2**
Systems Security Engineering
Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems
Final Publication: October 2018
- **NIST Special Publication 800-160, Volume 3**
Systems Security Engineering
Software Assurance Considerations for the Engineering of Trustworthy Secure Systems
Final Publication: December 2019
- **NIST Special Publication 800-160, Volume 4**
Systems Security Engineering
Hardware Assurance Considerations for the Engineering of Trustworthy Secure Systems
Final Publication: December 2020

NIST Special Publication 800-160, Volume 2

Systems Security Engineering

Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems

Public Comment Period

March 21 — May 18, 2018

<https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/draft>

Please send comments to sec-cert@nist.gov



CYBER RESILIENCY ENGINEERING FRAMEWORK

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

**100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930**

Email

ron.ross@nist.gov

LinkedIn

www.linkedin.com/in/ronross-cybersecurity

Web

csrc.nist.gov

Mobile

301.651.5083

Twitter

[@ronrossecure](https://twitter.com/ronrossecure)

Comments

sec-cert@nist.gov