Cyber Requirements Engineering

ITEA Emerald Coast Chapter
2018 Cyber Security Workshop
Cybersecurity: From Requirements to Test & Evaluation

PeopleTec
An Employee-Owned Company
People First. Technology Always.

Presented by:
Al Morris, CISSP, CHFI, CEH
Al.Morris@PeopleTec.com

Cyber Requirements Engineering

- **Confidentiality, Integrity and Availability (CIA): Tired, Worn out terms that have lost their meaning and significance after years of Information Assurance professionals preaching their importance**
- **Almost impossible to write good requirements specific enough to enable a system or product that will survive the extensive Cybersecurity testing or a real contested environment with these outdated goals driving your requirements**

Now What?

A New Triad is needed!

Prevent, Mitigate, Recover

- **Actionable Goals that truly indicate the functions of an effective Cybersecurity program**
- **Design your system / application with the goals of Preventing, Mitigating, and Recovering from the effects of a Cyber attack**
- **Providing the Confidentiality, Integrity and Availability of your information / system comes more naturally with these goals in mind**

What are the Goals of the Adversary in Regards to Your Information?

- **Deny access to information**
- **Modify the information**
- **Steal the information**

The effects of any one of these things happening to your information depends on what you are doing with it

You have to determine the value and use of your information.

What are Your Goals in Regards to Your Information?

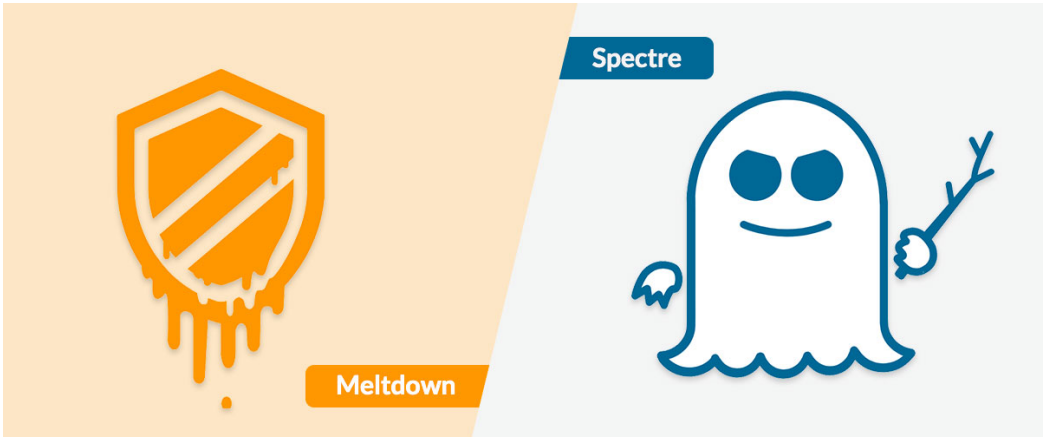
- **The primary goals of cybersecurity controls have implied secondary goals that cannot be overlooked. I.E. you can't *recover* from a cybersecurity incident if you can't *detect* one**
- **What speed and level of recovery is required for a system or application will depend on the function it provides**
- **If it's something like a medical device, an automobile, or aircraft that could affect someone's life, limb or eyesight both factors will be different than something that provides supply or logistics data**
- **What may be more important to a system or application processing supply or logistics data may be just the Integrity, in which case you want to *Prevent* data from being manipulated by authenticating the source and destination, and encrypting the data at rest and in transit which would fulfill the protection of the *Confidentiality* and *Integrity* of the information**

What are Your Goals in Regards to Your Information?

- **Only if the data was required to perform a critical function of the system or application would you need to be concerned with the *Availability*. If the data supports a critical function of a system or application that could affect someone's life, limb or eyesight additional design consideration need to be made**
- **Is the function critical enough that it would require hardware redundancy, or to the extreme of supplier diversity and redundancy to prevent a hardware or embedded software cybersecurity incident from affecting the critical functions?**
- **This criticality analysis effort could lead to further *Supply Chain Risk Management* and *Software and Firmware Assurance* design, contracting and testing requirements**

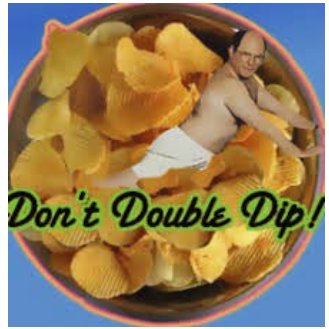
High Level Design Considerations

- **System of System design considerations and requirements need to be developed with the highest level of assembly in mind**
  - A low likelihood, low impact, low probability vulnerability in one non critical component of a system or application can be exploited and bring down critical functions if systems are designed and thrown together in stove pipes that will be tested only when the entire project is complete



Use Industry & DoD Standards

- Radio Technical Commission for Aeronautics (RTCA) DO-178 Software Consideration in Airborne Systems and Equipment Certification
- RTCA DO-326 Airworthiness Security Process Specification
- SAE International J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- Vehicular Integration for C4ISR/EW Interoperability-VICTORY
- Future Airborne Capability Environment – FACE
- Safety - governed by Army Regulation 385-10
- Airworthiness - governed by Army Regulation 70-62 and guided by MIL-HDBK-518B



No Seriously - Don't Double Dip

Cybersecurity ≠ Safety ≠ Airworthiness ≠ DO-178 ≠ FACE ≠ VICTORY

- **Each of these disciplines are mutually exclusive, but can still be complimentary to each other**
  - Example: An aircraft can pass all Cybersecurity, Airworthiness, DO-178C, and FACE requirements, but if every time the pilot lowers the seat it smashes his fingers, it won't pass the Safety requirements
- **The FACE standard maps to approximately 96 Cybersecurity controls, DO-178 can map to another 100 or so Cybersecurity controls. However a new system under development may have over 2000 security controls assigned to it, based on its System Classification under the Risk Management Framework**
- **Where we have a chance to reduce development costs & time with all of these different sources of requirements is by looking at the controls / requirements that overlap the disciplines and reuse the test results and documentation across each discipline**

Cross Reference the Standards

DO-178C		NIST SP 800-53 REV4	
Software Configuration Management Process Activity	**Reference**	**Control Number**	**Control Name**
Change Control - integrity and identification	7.2.4.a	CM-3	Configuration Change Control
	7.2.4.b	SA-10	Developer Configuration Management
Change Control - tracking	7.2.4.c	SI-7	Software, Firmware, and Information Integrity
	7.2.4.d	CM-3	Configuration Change Control
Change Review	7.2.4.e	CM-3	Configuration Change Control
	7.2.5	SA-10	Developer Configuration Management
Configuration Status Accounting	7.2.6	MP-4	Media Storage
Retrieval	7.2.7.a	CM-2(3)	Baseline Configuration | Retention of previous configurations
Protection against Unauthorized Changes	7.2.7.b.1	CM-5	Access Restrictions for Change
		CM-6	Configuration Settings
		CM-7	Least Functionality
		CM-9	Configuration Management Plan
		SA-10	Developer Configuration Management
		SA-12	Supply Chain Protection
		SA-15	Development Process, Standards, and Tools
		SC-28	Protection of Information at Rest
		SI-1	Information System Monitoring
		SI-7	Software, Firmware, and Information Integrity
		PE-3	Physical Access Control

Reuse & Reduce

- **Plan for the certification of each standard through the development life cycle**
- **Write into the requirements deliverables from one discipline that will cover another one**
  - I.E. NIST 800-53 control CM-3 is covered by three separate paragraphs in DO-178 compliance
    - DO-178 testing will be accomplished prior to RMF testing
    - Requirements for compliance with CM-3 will not be written into the Cybersecurity portion of the contract, just the artifacts from the DO-178 testing
- **Reduce testing time = WIN**
- **Reduced costs = WIN**

How do we Accomplish This?

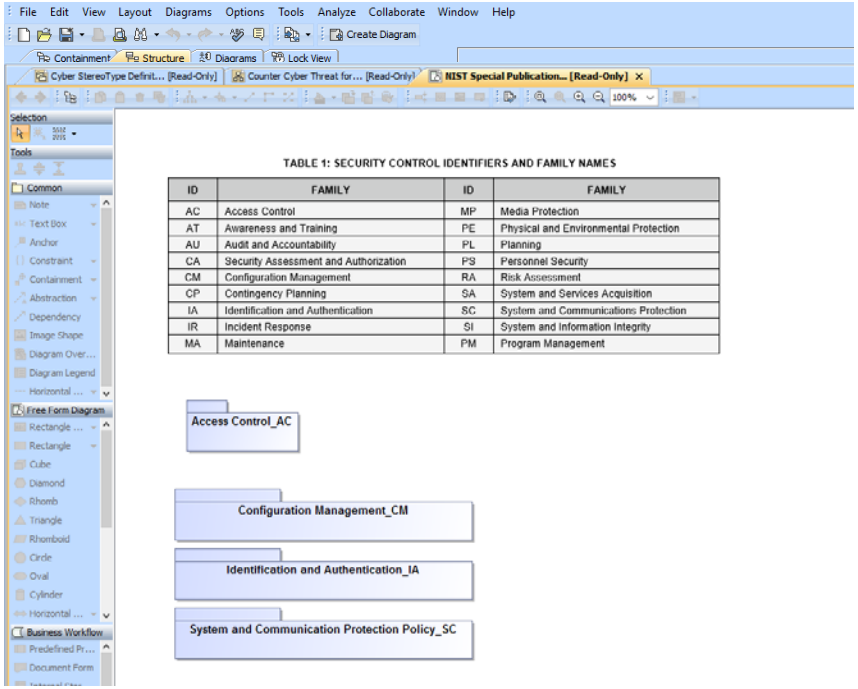
- **Meetings of course!**
- **Cybersecurity Engineers, Design Engineers, Safety Engineers, all the disciplines sit down together and cross walk the standards applicable to your program**
- **Write your requirements effectively to cover all disciplines without duplicating them**

The Results of the Meetings

Control Numb	Fam	Control Title	Control Text	Preven	Mitigat	Recov	Inherited/Planned/ or NA	NA Justification / Inherited Source	Army Recommendations/Comments	Discriminato
CM-2 (1)	CM	BASELINE CONFIGURATION | REVIEWS AND UPDATES	The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades.	X			Planned	DO178 section 4.1.g		
CM-3 (4)	CM	CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE	The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element].	X			Planned		ISSM/ISSO will be a member of the CM board when it starts.	
CM-3 (6)	CM	CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT	The organization ensures that cryptographic mechanisms used to provide [Assignment: organization-defined security safeguards] are under configuration management.				Planned			
CM-4	CM	SECURITY IMPACT ANALYSIS	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.		X		Planned		ISSM/ISSO will be a member of the CM board when it starts.	X
CM-5	CM	ACCESS RESTRICTIONS FOR CHANGE	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	X			Planned	DO-178 Section 7.2.7.b.1		
CM-5 (5)	CM	ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES	The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment; and (b) Reviews and reevaluates privileges [Assignment: organization-defined frequency].	X			Planned	DO-178 Section 7.2.7.b.1		
CM-5 (6)	CM	ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES	The organization limits privileges to change software resident within software libraries.	X			Planned	DO-178 Section 7.2.7.b.1		

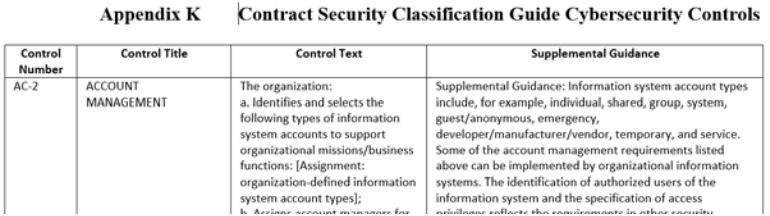
What do You do with These Results?

- **Be an Engineer, not just a Cyber Geek!**
- **Collaborate, use real engineering tools to embed Cybersecurity into the System Design**
- **Categorizing the controls as activities, and defining the functions they provide, (PMR) makes this task easier**



What You End Up With

- Cybersecurity
- Cooperative Vulnerability Assessments
- Adversarial Cybersecurity
- Cybersecurity Assessments
- CS Management Plan
- Disposition of Data
- Program Protection Implementation Plan
- Product / Application Cybersecurity Controls*



Appendix K Contract Security Classification Guide Cybersecurity Controls

Control Number	Control Title	Control Text	Supplemental Guidance
AC-2	ACCOUNT MANAGEMENT	The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];	Supplemental Guidance: Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access

* “The cybersecurity controls for System X shall be IAW SOW Appendix K. The contractor shall provide alternate mitigating controls or provide language to support removing a control subject to USG approval that will be documented in the minutes of the CS WG”

You’re not done yet!

Source Selection Evaluation Board

- **Tell them what is important to your program!**

Evaluation Criteria: Note: These controls are just 22 of the 80+ controls in the EMD contract and were selected because they affect the Cybersecurity KPP and/or the guidance from the JCIDS Manual.
Acceptable – the Offeror displays a mastery in their proposal of all the "Prevent Controls" listed in table below.
Good – the Offeror displays a mastery in their proposal of all the "Prevent and Recover Controls" listed in the table below.
Outstanding – the Offeror displays a mastery in their proposal of all the "Prevent, Recover and Mitigate" listed in the table below.

Control Number	Family	Control Title	Control Text	Prevent	Mitigate	Recover	Comments
AC-3	AC	ACCESS ENFORCEMENT	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	X			
AC-3 (4)	AC	ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL	The information system enforces [Assignment: organization-defined discretionary access control policies] over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following: (a) Pass the information to any other subjects or objects; (b) Grant its privileges to other subjects; (c) Change security attributes on subjects, objects, the information system, or the	X			

The CSMP shall include how the Contractor and subcontractors safeguard DoD CUI using the security controls in NIST SP 800-171. The CSMP shall document the process of reporting cyber incidents in accordance with paragraph (c) of DFARS 252.204-7012.

Evaluation Criteria: Outstanding – The CSMP address' each of the controls listed in NIST SP 800-171 without tailoring and controls. Acceptable – Controls have been tailored out (Requires CIO G-6 approval) Checklist provided below.

Control #	Control Title	CSMP
AC-2	Account Management	
AC-3	Access Enforcement	
AC-17	Remote Access	

Related Reading

- **The Joint Staff J-8 has posted the Cyber Survivability Endorsement Implementation Guide and several other SS KPP-related documents on NIPR Inteldocs:**

- **https://go.intelink.gov/fr5iAbI**

- **The site requires a CAC and Intelink account to access**

Conclusion (TLDR)

- **Do Cyber (right)**
  - Include everyone!
- **Classify your information**
- **Determine the protections needed**
- **Reduce cost & time (overlap)**
- **Actionable Requirements/goals**
- **Provide guidance to SSEB**
- **Seriously CSEIG is a good read – look for it if you have access!**

Questions?