CSIAC Cyber Security & Information Systems
Information Analysis Center

Basic Center Operations (BCO)

FA8075-12-D-0001

CSIAC REPORT:
Defense Acquisition University Secure Systems Design Course Experiment
Jun 2017 (Quarter 3)

This Final Report is delivered by the CSIAC BCO to document the results of the “Defense Acquisition University (DAU) Secure Systems Design Course Experiment” during the third performance quarter of 2017. The Cyber Security and Information Systems Information Analysis Center (CSIAC) is operated by Quanterion Solutions Incorporated.

Approvals:

Michael W. Weir

______________________________ Date ______10/10/17_______

Michael Weir, CSIAC Director

______________________________ Date ______10/10/17_______

Timothy Denman, DAU Cybersecurity Director

CSIAC is operated by:

QUANTERION
SOLUTIONS INCORPORATED

266 Genesee St.
Utica, NY 13502

Table of Contents

1 Executive Summary

The Cybersecurity and Information Systems Information Analysis Center (CSIAC) developed a course experiment with the Defense Acquisition University (DAU) Cybersecurity Enterprise Team which was executed on 17-18 May 2017. The goal of this exercise was to study the techniques and strategies used to provide cybersecurity-based training, in an effort to educate the entire acquisition workforce (all career fields/positions) to apply cybersecurity best practices and techniques. In collaboration with DAU and George Mason University (Arlington, VA), CSIAC hosted a total of 24 acquisition professionals and educators to participate in the Cybersecurity Secure Design Workshop. Day 1 was facilitated by CSIAC and DAU staff and included excellent participation and insight from acquisition practitioners. The learning objective for was to "Identify cybersecurity principles that must be considered throughout the acquisition lifecycle." Participants from the Navy, Air Force, Army and industry were asked to identify cybersecurity issues that related specifically to their organizations. They were then broken into small groups and asked to work through a related cybersecurity case study at different stages of the acquisition lifecycle. Day 2 consisted of educators from DAU, CSIAC, and George Mason working through participant responses and identifying training gaps and the needs of the acquisition workforce (see Appendix B for details). Additional workshops, cybersecurity articles, and jointly authored curriculum are expected outputs of this workshop. A plan of action was developed and a road map was created for all action items. Comments from practitioners were extremely positive and a strong working relationship between DAU, CSIAC and George Mason was developed. The key findings from this workshop are included below.

Key Workshop Findings

(See Section 3 for details)

1. **Establish Formal Cybersecurity Requirements Early in The Acquisition Life Cycle**
2. **Tailored Cybersecurity Training is Required for Each Area of Acquisition**
3. **Cross-Competency Unified Cybersecurity Perspective is Paramount**
4. **Senior Leader/Resource Management Cybersecurity Training & Education is the Critical Area**
5. **Cyber should be Considered As Any Other Systems Engineering Competency**
6. **Increased Weapon System and Operational Technology (OT) Training is Needed**
7. **Beware of Applying General Information Technology (IT) Cybersecurity to an OT Problem**
8. **Formalized Accountability For Cybersecurity Risk must be Enforced**
9. **Prioritized, Simplified & Integrated Cybersecurity Policy & Standards are Lacking In Current Acquisition Methodology**

2 Background

CSIAC developed a course experiment with the DAU Cybersecurity Learning Director, Timothy Denman, which was executed on 17-18 May 2017. The goal of this exercise was to identify gaps in DAU curriculum related to cybersecurity in the acquisition life cycle. This effort served a larger goal to better educate the entire acquisition workforce (all career fields/positions) to apply cybersecurity best practices and techniques early on in the acquisition process, strengthening secure system design, increasing survivability, and reducing expediential cybersecurity costs once fielded.

The vision driving this initiative consists of two basic principles:

- Identify cybersecurity principles that must be considered throughout the acquisition lifecycle
- Provide education and training to the acquisition workforce that facilitates the DOD cybersecurity mission through the acquisition life cycle and across career fields, leading to improved acquisition outcomes

After careful consideration, coordination and planning, the goals of this exercise include the following:

- Identify key gaps in current cybersecurity Training and Education at DAU
- Develop an understanding of how cybersecurity policy applies to the system acquisition life cycle, and which specific policies apply
- Given a notional system, choose key life cycle decisions that meet both operational and security objectives

3 Key Findings and Actions

The overall purpose of this experiment was to provide an environment for a group of acquisition SMEs to walk through an acquisition scenario to extract key cybersecurity areas that need to be addressed in DAU curriculum. Below are the key findings that should be considered during future curriculum approaches and development:

1. **Establish Formal Cybersecurity Requirements Early in The Acquisition Life Cycle** Even though this is not a new concept, acquisition professionals need to be made aware of this early in their careers through early training/education in order for it be realized in policy and practice. This will help acquisition professions to ultimately decide how to make the best decision between early requirements and the risk of going being too early in the process. There is also the high percentage of programs that are "legacy" and must be reconsidered far into sustainment where, as discussed, even simple fixes can have large time and funding needs. Early wargaming of the capability could be key to establishing a foundation of key requirements which can result in better prioritization and funding and save time and cost in the final phases of production/sustainment.

   Action: Research recent programs and provide Lessons Learned in all cybersecurity modules of test proven, critical and discreet cybersecurity requirements that should be in the ICD and draft CDD in the material Solution Analysis phase. JROCM Cybersecurity Survivability Attributes (CSA) as part of the System Survivability KPP are already being taught across DAU courses. Early use of Cyber Table Tops (CTT) can help to identify cybersecurity requirements and resultant architectural design.

2. **Tailored Cybersecurity Training is Required for Each Area of Acquisition Competency**
The main consensus of the participants was that even though there is a need for highly experienced cybersecurity professionals in acquisition, the acquisition community would be best served if all career fields received at least a knowledge level of training, so that they can apply their personal technical depth to the practical cyber context. Certifications and even college minor/concentration tracks could be used (with these requirements established in the formal job descriptions) for this purpose to supplement their specific area of expertise to provide adequate field representations when the highly trained cybersecurity specialists are not available/needed.

   Action: DAU has tailored Cybersecurity modules for ENG, TST, ACQ, LOG, ISA, Mission Assist and Leadership courses. However, CON and BCF need to be addressed.

3. **Cross-Competency Unified Cybersecurity Perspective is Paramount**
In order to achieve the main theme to develop formal requirements early, so they can be prioritized, planned and resourced, having multiple stakeholder career fields in the room, to include the intelligence and vulnerability assessment teams, all speaking the same language and working with a common goal early in the acquisition development cycle or recertification of legacy systems, is paramount to success. Both acquisition professionals, as well as cybersecurity SMEs, must be aware of each other's purpose and how they can work together to produce a survivable capability. This involves both being involved in decision boards early in the process and that the both looking toward the same goal. An example of this is how the Judge Advocate advises the Commander in the military. Their job is not to say "No," but work together to say "Yes" in a way that meets both operational and legal mandates. This concept should be taught across the board and leveraged into any similar training/education for effectiveness and efficiency.

   Action: Tailored courses and modules are approaching this concept, but there is a gap in a completely unified cross-competency approach that can be incorporated into in the Cybersecurity Awareness across DoD Acquisition Workshop

4. **Senior Leader/Resource Management Cybersecurity Training & Education is Critical**
Continuing on the perspective point, not only do multiple acquisition career fields need to be aware and involved, senior leadership who direct resource management and prioritize funding need to have an understanding of what cybersecurity will and will not buy them, so that we get the best, most survivable capability for the dollars spent.

   Action: DAU is emphasizing the cybersecurity modules in Senior Leadership courses and Defense Acquisition Executive Overview Workshops (DAEOW)

5. **Cyber should be Considered as Any Other Systems Engineering Competency**
Cyber Should Be Treated Like/Prioritized with All Other Parts of the Program – Even though cyber effects on weapon systems tend to be growing, cybersecurity requirements need to be developed and justified just like all other requirements of the system. However, this involves the community being adequately aware of how cybersecurity affects their systems, so that a true comparison/tradeoff of capability and protections can be developed and managed throughout the lifecycle.

Action: DAU has tailored Cybersecurity courses modules for ENG, TST, ACQ, LOG, ISA, Mission Assist and Leadership courses that specifically address Cybersecurity in context with Systems (Security) Engineering.

6. **Increased Weapon System and Operational Technology (OT) Training is Needed**
Even through some enterprise IT concepts and training can be leveraged for the acquisition community, there is a growing need for specialized training in operational technology (OT), also called PIT because of the formats and different operating concepts. This also involves curriculum needs in showing acquisition professionals the key concepts of PIT functions and their potential weaknesses from a hacking perspective. This also involves possibly new discussions like cyber instrumentation versus anti-tamper efforts. The participants understood that this more specialized training is an added cost, but that depth and breadth should be prioritized by job position, so that all the community can truly understand the environment to better prioritize cybersecurity vulnerabilities against system capabilities.

Action: DAU has introduced new Cyber Risk Assessment, Table Tops and FMECA concepts applicable to OT in ENG, TST, ACQ, LOG, ISA, Mission Assist and Leadership courses. There is a serious constraint in specific training that would be classified.

7. **Beware of Applying General Information Technology (IT) Cybersecurity to an OT Problem**
Beware of Applying IT Cybersecurity to a OT Problem Set – Even though all capabilities should be risk managed against cybersecurity vulnerabilities, there are some mostly enterprise IT based controls that may not directly transfer to OT/PIT scenarios and may, in fact cause less mission effectiveness and survivability in the long run. An example discussed was the consideration of using CACs in cockpits. While this approach seems to be an overall effective tool in an enterprise IT environment it may not make sense, or be counterproductive, in an operational environment. The key point is that acquisition professionals must be trained and educated on both, so that this gap can be bridged with critical thinking, thoughtful management, and even possibly new RMF template development to increase efficiency.

Action: Also, being taught as per above, but lacking a better exercise and exemplar directly applicable to a weapon system other that an automobile hack and the Wright Flyer.

8. **Formalized Accountability for Cybersecurity Risk must be Enforced**
Along with providing informed/deliberate funding of formal, up front requirements, senior organizations on down must be trained/educated how to inspire and hold accountable acquisition professionals to hold to requirements and standards. This could be leveraged with existing courses to include educating on the consequences of not considering cybersecurity, as well as inspiring/showing them how combined efforts from multiple backgrounds can truly result in the most survivable capability possible.

Action: DAU cannot enforce this, although it is being taught as per DoDI 5000.02

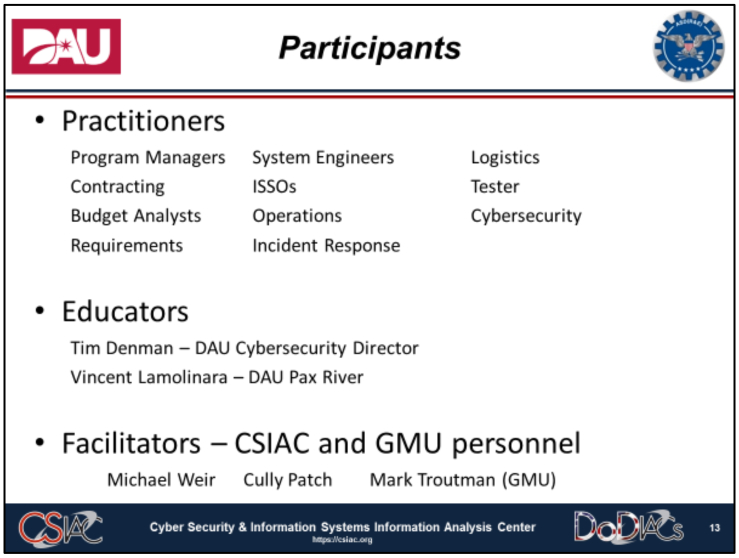
9. **Prioritized, Simplified & Integrated Cybersecurity Policy & Standards are Lacking in Current Acquisition Methodology**

Key gaps exist trying to make sense of not only the multiple accreditation processes, of which several could be needed in a program at once, but how to untangle and most importantly, make useful, the large amount of cybersecurity policy and standards, mandates and guidance. This is key in developing both prioritization and leveraging doctrine/lessons learned to make the best use of time and funds spent to get the best capability.

Action: DAU is able to see across many DoD and Service initiatives and is uniquely able to support the Cyber Technical Advisory Group and special workshops such as the MITRE Cyber Weapon System Resiliency effort and will continue to do so and incorporate new standards.

4 Participant Backgrounds

In order to provide multiple perspectives to the experiment, many participants were invited across several career fields. On the day of the experiment, in addition to the DAU/GMU stakeholders and CSIAC facilitators, 13 acquisition professionals attended, ranging from Program Managers (PMs) to logistics, operational test and evaluation (OT&E), and sustainment professionals, as well as members with extensive contracting experience and avionic security vulnerabilities expertise. Each of the participants had an established background in the acquisition field, with about half having prior military operational experience (see Figure 1). The contributors were asked to fill out a DAU Secure System Design Course Experiment Data Sheet to document their background/perspective for later analysis (see Appendix G).



Participants

- Practitioners

  Program Managers
  Contracting
  Budget Analysts
  Requirements
  System Engineers
  ISSOs
  Operations
  Incident Response
  Logistics
  Tester
  Cybersecurity

- Educators

  Tim Denman – DAU Cybersecurity Director
  Vincent Lamolinara – DAU Pax River

- Facilitators – CSIAC and GMU personnel

  Michael Weir   Cully Patch   Mark Troutman (GMU)

Cyber Security & Information Systems Information Analysis Center
https://csiac.org
13

Figure 1: Exercise Facilitators and Participant Backgrounds

5 Assumptions

The objectives of this exercise were not focused on convincing the participants of the importance of cybersecurity; this shared notion is what drove these professionals' interest in the experiment. Instead, the assumptions were based on recent statements and guidance from DoD. The participants focused on the identification of the current training gaps and possible solutions through which they could be eliminated.

- **Central Theme:** No cybersecurity equals mission impact
  - In a cyber contested environment
- "All our efforts to improve technological superiority will be in vain if we do not provide effective cybersecurity throughout the product lifecycle."
  - **Reference:** "Implementation Directive for Better Buying Power 3.0 – Achieving Dominant Capabilities through Technical Excellence and Innovation – April 9, 2015"
- "The Defense Acquisition University curriculum [will be] updated to reflect … cybersecurity considerations and requirements for all of the career fields."
  - **Reference**: "Improving Acquisition from Within," Suggestions from our Program Executive Officers (PEOs), Mr. Frank Kendall, Defense AT&L: July – August 2016

6 Participant Concerns

The participants had a number of initial concerns that were expressed both during the introductions, as well as throughout the experiment. A summary of the issues discussed is provided (see Table 1):

Table 1: Main Initial Concerns Summaries

Initial Concern
1. Implementing NDAA 1647 mandates on weapon system vulnerability assessments
2. Cyber impacts affecting foreign sales partners
3. Cyber technical requirements not in program requirements to Operate (ATO) vs effective cybersecurity
4. Design cyber in vs. reviewing at a milestone
5. Time constraints prevent detailed cyber training
6. What's necessary to provoke more cyber training
7. DoD needs to incentivize cyber training
8. Cost of constantly evolving compliance standards
9. Programs need to define Confidentiality, integrity and Availability (CIA) objectives at onset
10. Cyber SMEs not included in acquisition process
11. Combining physical and information security
12. Defining security boundaries
13. Compliance for Authority
14. Inadequacy of cyber intelligence for NDAA 1647
15. Inadequacy of NIST 800-53 / 160 security controls and system security engineering (SSE) for military systems
16. Unfunded cybersecurity mandates
17. Should focus on legacy systems

Initial Concern
18. Cyber solutions must be ‘retrofittable’ to legacy systems
19. DoD PM guidance for RMF lacks impact on production
20. Too much focus on Defense Business Systems (DBS)
21. RMF & DBS mindset can increase cost and decrease security
22. Wasted effort in justifying non-compliance with inappropriate security controls
23. Knowledge gap due to security classification of cyber vulnerabilities
24. Unbounded Red Team assessments not realistic
25. Non-Internet Protocol (IP) cyber attacks, i.e., 1553 databus
26. No database of weapon system cyber attacks
27. No simple fixes – cybersecurity will delay programs

A more detailed account of the participants’ cybersecurity related concerns for the acquisition community is provided by the corresponding numbers in Table 1A in Appendix A.

7 Main Experiment (Day 1 – 17 May 17)

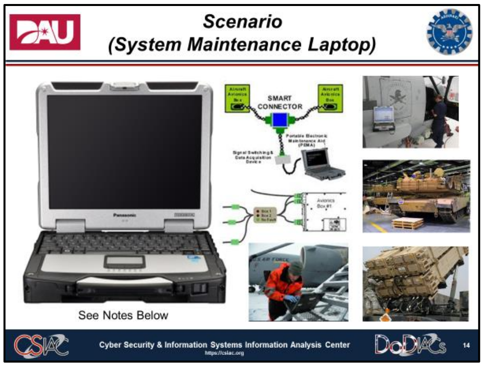
The experiment was structured as a collaborative walk through of a real-world exemplar of the acquisition process. The general motivation for this format was to collectively step through the acquisition cycle, focusing on specific milestones to reveal critical gaps in cybersecurity knowledge or experience that prevents acquisition professionals from being able to secure their systems while meeting mission and budget requirements.

7.1 Introduction

To remain dynamic, and achieve the objectives of the experiment, the facilitators had a brief discussion with the participants to get a feel for which milestone would be most appropriate for the experiment’s break out session. The general consensus was to primarily address the legacy/upgrade, but to also balance that discussion with the newly developed systems milestone. Each breakout included three teams.

- The first breakout walked through Post-Milestone A – Pre-Milestone B, and was grouped by career field where participants had to role play multiple professions/responsibilities.
- The second breakout walked through Post Milestone B, Pre-Milestone C and was more randomly distributed, providing a wider variety of perspectives to work through the issues.

An upgrade/reauthorization under the Risk Management Framework (RMF) for a maintenance laptop (sometimes referred to as a Portable Electronic Maintenance Aid (PEMA)) was used as the representative system to follow through the scenario (see Figure 2). This was chosen not only because it is an example of a pre-existing system, but because it is a key interface to aircraft and other weapon systems. These laptops provide an electronic technical reference and can represent a loader for other devices that interface with Enterprise IT, as well as having the potential to directly interface with the aircraft to update software, mission data, etc.



Scenario
(System Maintenance Laptop)

See Notes Below

Cyber Security & Information Systems Information Analysis Center
https://csiac.org

14

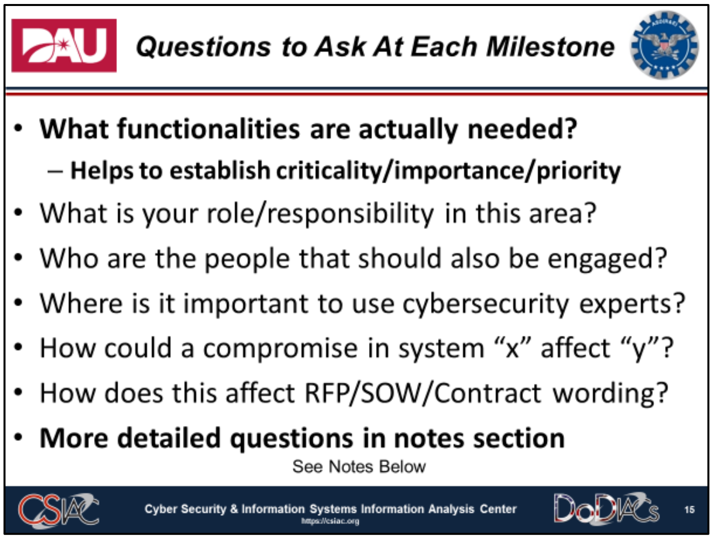
Figure 2: Maintenance Laptop Scenario

Prior to the team breakouts, the participants discussed a number of general considerations. Concepts/questions included the following (see Table 2):

Table 2: General Considerations Prior to Experiment

What is the user population?	What are these computers being used for? Reference? Loaders? Tester?	How severely does it impact us from test set functions to technical order/publication retrieval?
How are different generations affected (i.e. the newer generation tends to use these devices almost exclusively for troubleshooting, etc.)?	How much will it degrade your system?	What are the effects if it is taken out?
Does it ground the aircraft in some way?	How much longer will it take to troubleshoot a degraded system?	Does it effectively scrub a mission because we miss a flight?”
What is it connected to (wireless back to the aircraft maintenance unit (AMU), the aircraft, etc.)?	What’s the level of the data? Who is the owner of the data? (DIA?/GENSER?)	What assessment and authorization methods does this drive?

The facilitators divided the participants into three groups and asked each group to define the acquisition process to a level of confidence for the group as they followed the scenario through the chosen milestone. The scenarios were purposefully loosely defined with the expectation that each group would form different assumptions, starting points, boundary conditions, etc. as part of this discovery process. Facilitators went on to reference the established questions (see Figure 3 and more detailed questions in Appendix D) to provoke the necessary analysis, while also addressing the related policy and guidance tools that should shape the acquisition process (see Appendix E).



Questions to Ask At Each Milestone

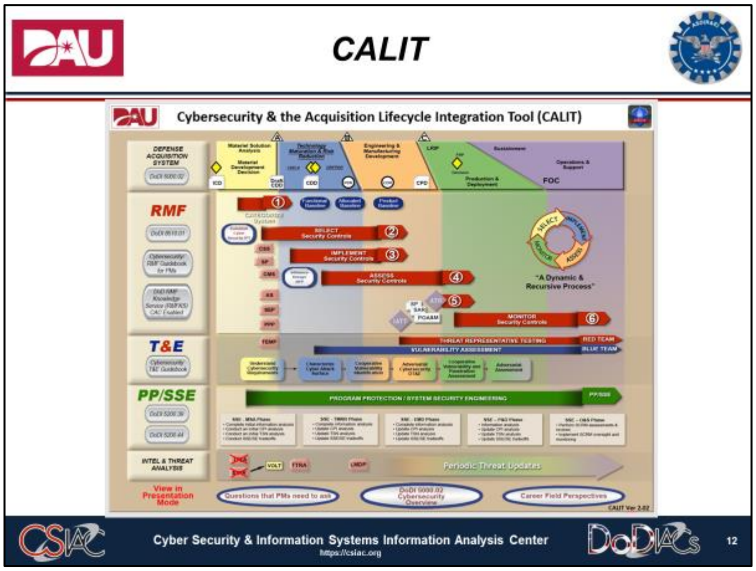
- **What functionalities are actually needed?**
  - **Helps to establish criticality/importance/priority**
- What is your role/responsibility in this area?
- Who are the people that should also be engaged?
- Where is it important to use cybersecurity experts?
- How could a compromise in system "x" affect "y"?
- How does this affect RFP/SOW/Contract wording?
- **More detailed questions in notes section**

See Notes Below

Cyber Security & Information Systems Information Analysis Center
https://csiac.org
15

Figure 3: Main Questions (Detailed Question in Appendix C)

Breakout #1 Focused on Post Milestone A - Pre-Milestone B (Upgrade), using the "Cybersecurity and the Acquisition Lifecycle Integration Tool (CALIT)" (see Figure 4) as a roadmap for the activities to be performed. The teams were organized by career field. The facilitators also provided a small list of references that may be of use during the experiment (see Appendix I).



CALIT

Cybersecurity & the Acquisition Lifecycle Integration Tool (CALIT)

DEFENSE ACQUISITION SYSTEM
DoDI 5000.02
Material Solution Analysis
Material Development Decision
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
LRIP
Sustainment
Production & Deployment
Operations & Support
FOC
ICD
Draft CDD
CDD
CPD
RMF
DoDI 8510.01
Cybersecurity RMF Guidebook for PMs
DoD RMF Knowledge Service (RMF KS) CAC Enabled
SELECT Security Controls
IMPLEMENT Security Controls
ASSESS Security Controls
MONITOR Security Controls
SELECT
IMPLEMENT
ASSESS
MONITOR
"A Dynamic & Recursive Process"
POA&M
T&E
Cybersecurity T&E Guidebook
THREAT REPRESENTATIVE TESTING
RED TEAM
VULNERABILITY ASSESSMENT
BLUE TEAM
PP/SSE
DoDI 5200.39
DoDI 5200.44
PROGRAM PROTECTION / SYSTEM SECURITY ENGINEERING
INTEL & THREAT ANALYSIS
Periodic Threat Updates
View in Presentation Mode
Questions that PMs need to ask
DoDI 5000.02 Cybersecurity Overview
Career Field Perspectives
CALIT Ver 2.02

Cyber Security & Information Systems Information Analysis Center
https://csiac.org
12

Figure 4: Overview of the CALIT

The scenario objectives were to walk through the development of an Initial Capabilities Document (ICD), Capability Development Document (CDD) and Preliminary Design Review (PDR) while trying to mature the design and work through risk reduction and RMF controls. The participants attempted to select controls, implement them, and assess them all at the same time. They characterized the attack surface, intelligence requirements, and system security engineering practices, all while considering Critical Program Information (CPI) and Trusted Systems and Networks (TSN) while not yet knowing all of the related factors.

While thinking through the Technology Maturation and Risk Reduction (TMRR) Phase, the participants were reminded to consider the several guidance documents and to use them as a tool to guide the process. They started thinking about some of the questions such as what data they needed, how important it was, who were the data owners, etc. all while pursuing the ultimate goal of identifying the necessary cybersecurity knowledge and skills to update the current training curriculum.

7.2 Breakout Session #1 – Out Brief (In the order that were briefed)

For this breakout session, the teams were assigned the following responsibilities.

- **Team #1 (Contracts/PMs)** – Focused more directly on answering the main questions first with discussion.
- **Team #2 (Test and Engineering) -** Framed the answer in terms of confidentiality, integrity, and availability (CIA).
- **Team #3 – (Logistics)** – Focused on logistician portions of the problem and summarized based on what had already been covered by the previous two other teams.

Below is a list of questions addressed by each team:

Table 3: Breakout Session #1 Questions Addressed by Team

Questions	Tm 1 Contr & PM	Tm 2 Test & Eng	Tm 3 Log
1. What functionalities are actually needed?	X	X	
2. What is your role/responsibility in this area?	X	X	X
3. Who are the people that should also be engaged?	X	X	
4. Where is it important to use cybersecurity experts?	X	X	
5. How could a compromise in systems “x” affect system “y”?	X	X	
6. How does this affect RFP/SOW/Contracting wording?	X	X	
7. A lot of people are going to need to support you to get this task done, is there that much [cybersecurity] talent available out there?	X		
8. If you had to cut 10% out of your budget for cybersecurity how would you do that?	X		
9. Has anyone ever seen a prioritized list of cybersecurity requirements?	X		
10. What are you, after you went through this, what’s the thing you are most worried about in this stage [cyber domain Pre-Milestone B]?	X		
11. Are there PEOs or Program Management Agreements (PMAs) involved in this?	X		
12. Can you act as program manager even if you haven’t been officially designated?	X		
13. What about PBL [Performance-Based Logistics]?			X
14. What happens when things become obsolete? Are these planned into the ACQ lifecycle?			X

Questions	Tm 1 Contr & PM	Tm 2 Test & Eng	Tm 3 Log
15. If I can do something to your data, do you care about that? Even in a gradual manner such as changing the number of engine cycles to increase engine changes. Is anyone worried about that?			X
16. What is your worst worry given the cyber scenario?			X

Below is a summary of the results/briefs of each team:

Table 4: Breakout Session #1 Finding Summary

Team #1 – Contracts/PMs	Team #2 – Test & Engineering	Team #3 – Logistics
Cyber is not a special competency all its own; it is integral to traditional competencies such as engineering, test, & sustainment	Security requirements need to be considered, so the information can flow in the required channels (Unclassified, Secret, etc.)	Logistics is very important up front as it can consider long-term, manning training and other long-term sustainment
All roles have a part to understand the impacts of cyber on their roles and to provide the same teaming and coordination needed to assess tradeoffs with other parts of the system	Impact of information loss or alteration must be assessed to impact early in order to establish the appropriate resiliency levels	Just like all other parts of the system, must decide whether to sustain in-house or go with a Contractor Logistics Support (CLS) strategy, noting tradeoffs for both
The whole integrated product team needs to consider cybersecurity requirements up front as the impacts affect everything from design to logistics	User population must be thoroughly understood, so that the vulnerabilities/impact of data loss/alteration are considered	Information flow security from source to system must also be considered in CLS vs. in-house strategies
Cybersecurity expertise must be considered during alternative analysis, as well as contracting to ensure realistic impact assessments and costing	Specification refinement can be key to minimizing to only needed software and upgrade planning	Performance-based Logistics must also be considered for cybersecurity equities
Need to consider cybersecurity requirements/impacts up front to help save cost and schedule loss	Cybersecurity interface with system architects and RMF personnel is critical to overall system success	Key wins can be considered by long-term thinking, especially how updates can securely, yet efficiently occur throughout the lifecycle
Must try to quantify effectiveness/mission impact	Cybersecurity needs to be considered for the entire	Must also consider in CLS when technology enters

Team #1 – Contracts/PMs	Team #2 – Test & Engineering	Team #3 – Logistics
as much as possible in order to effectively balance tradeoffs for an acceptably resilient system	lifecycle; from development to disposition of possibly sensitive design and operational information	obsolescence if it will still be supported
Cyber requirements/impacts must be listed as early as possible to identify interdependencies, as well as support tradeoffs with other system requirements/impacts	Mission impact to the data used needs considering to determine the level of data handling & validation necessary to manage the risk	Clear consensus and language with stakeholders, including contractors, is key to developing/sustaining a resilient capability
Cybersecurity must be defined, manned, equipped, and sustained in line with all other requirements of the system	Early perspectives/buy-in from stakeholders is key to building adding resiliency to the required capability	Higher classifications of data must be balanced with the cost and shareability of mission critical data

The participants' detailed responses to the question sets for Breakout Session #1 are provided in Appendix C: Breakout Session #1 Question/Answer Detail, Tables 4A, B, and C. Those interested in a more concise summary are encouraged to consult Section 3.

7.3 Post Breakout Session #1 Discussions

The post breakout #1 discussion not only brought some conclusive thoughts, but questions having to do with training/educating the workforce to be most productive (see Table 5).

Table 5: Post Breakout Session #1, Group Discussion Summary

Requirements establishment as early as possible reigned supreme	There are other information support dependencies/mediums to consider such as radio frequency/optical transmissions and their tradeoffs
Documentation needs to be properly prepared from the start in order to best provide effective risk management	Must educate stakeholders on why cyber-security testing is a way to cooperatively develop more resilient capabilities
Development/Access to your interface control document (ICD) is critical in order to coordinate cybersecurity dependencies/interactions to best make the tradeoff decisions through the life cycle	Leads to consider how division of labor should occur. Should we make some engineers cybersecurity experts or make some cybersecurity experts system engineers?
Viewing software code versus having just the product/service provided must be considered when considering the ability to evaluate risk	How should career field managers ensure that their workforce has the right balance of cybersecurity in order to be effective?
Early test and evaluation is necessary in order to catch issues when they can be relatively easily corrected	How do transitions from Government to private, or cross-career field changes affect the process?

The participants' detailed responses are located in Appendix D, Table 5A.

7.4 Breakout Session #2

This break out session used the same scenario as the first session, but concentrated on **Post Milestone B, Pre-Milestone C.** The groups were also changed, this time consisting of participants from different career fields in order to provide wider perspectives (see Table 6).

- **Team #1 (Post Milestone B, Pre-Milestone C Focus)** – Focused on the PEMA just before low-rate initial production (LRIP).
- **Team #2 (Post Milestone B, Pre-Milestone C Focus)** – Focused on open ended questions that were discovered during the walk through.
- **Team #3 (Post Milestone B, Pre-Milestone C Focus)** – Focused on logistician portions of the problem and summarized based on what had already been covered by the previous two other teams.

Table 6: Breakout Session #2 Finding Summary

Team #1	Team #2	Team #3
Need to freeze the baseline at the Critical Design Review (CDR) to prevent scope creep until LRIP/spiral, etc.	Cybersecurity requirements must be periodically reevaluated throughout development/lifecycle	Must get ATO at this stage, verification of the cyber table top and cyber risk assessment are key
Ensure to include all stakeholders, including legal, to ensure all perspectives are considered for contracting development through sustainment	Operational testers should evaluate systems during the developmental stage to identify issues that can be fixed before production	Need to review the POAM, ATO, or ITT to identify issues that will need to be funded/scheduled prior to production as well as any needed contract wording changes
Everyone needs to be trained/educated in cybersecurity and how it affects the value they provide in their career field/position	Cybersecurity must be considered cross-domain in order to evaluate and manage cybersecurity risks	Must understand the requirements, threats, and risks to the program and balance them with mission success and survivability
Impacts of key systems such as the mission computer must be considered for cybersecurity to be balanced with not placing security features in places where it may cause mission failure itself (e.g. CAC insertion in order to operate aircraft)	Software minimization is key on the PEMA as each software part introduces inherit risk of a wider cyber footprint, which can be eliminated if it is not needed for the mission	It is key to perform the cyber risk assessment as early as feasible in order to support effectiveness/survivability tradeoffs with other parts of the over system capability
If contracted, need to decide the best vehicle based on the requirements and integration with the system capabilities (e.g. tech specific or objective based)	The use of “orange” or out-of-band instrumentation should be considered for cyber systems as a backstop to indicate system compromise and attempt remediation prior to mission impact	

The participants' detailed responses to the question sets for Breakout Session #2 are provided in Appendix E, Tables 5A, B, and C. Those interested in a more concise summary are encouraged to consult Section 3.

8 Hot Wash (After Action Report) and Final Comments

This portion was a final chance for the participants to provide comments/feedback having gone through the entire experiment (see Table 7).

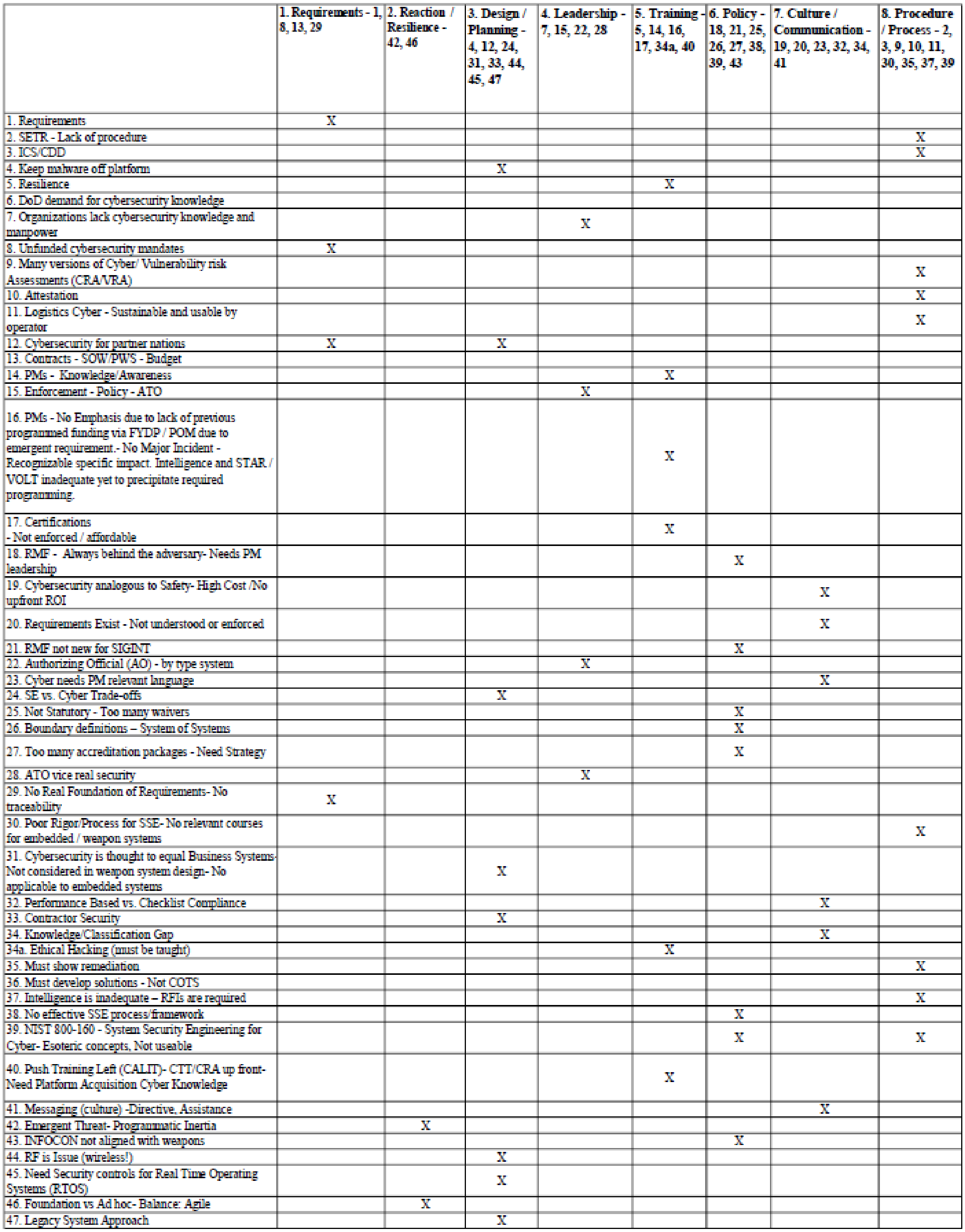
Table 7: Hot Wash (After Action Report) Summary Bullets

Learned a great deal about other career field perspectives on cybersecurity; very eye-opening	I admire the technical testers/red teams that try to provide good feedback to the acquisition community
On the core competency issue (whose responsibility is it to do what in cybersecurity), suggest an additional specifier in logistic and other career fields to certify in cybersecurity related to their job for overall workforce effectiveness/success	There is much to understand for all stakeholders in the platform information technology (PIT)/Operational Technology (OT) side of weapon systems as many information technology (IT) solutions don't apply
DAU has a very important function in effecting mission resiliency through workforce development in cybersecurity	Need to understand the data owners, accrediting authorities, user population, and levels of concern in order to design security architectures effectively
While cyber table tops can be helpful, the should not be mistaken of substituted for the systematic rigor of a cyber vulnerability assessment, as it is key, with all other points described during the experiment, so program managers can make key decisions during development and beyond	Cybersecurity needs to be a cross-domain, working group focused endeavor in order to learned and implemented across the many areas where it applies
Would like to see continued visibility on how DAU curriculum may change in addition to suggest creating a dual major and/or at least a minor in acquisition career tracks to help establish the required competencies for cyber related positions	Critical thinking in cybersecurity is an absolute must and that we must look at it a little different in the way we build classes, perhaps more toward cross-functional workshops such as this experiment

The details of this discussion can be found in Appendix F, Table 7A.

9 Initial Findings (Day 2 – 18 May 17)

The next day, educators and facilitators came together with the previous day's capture/documentation and performed some initial data reduction. What resulted was a 47-item list of prioritized issues along with a general category heat map to start to bring them together (see Figure 5 below, and Appendix B for details).



	1. Requirements - 1, 8, 13, 29	**2. Reaction / Resilience - 42, 46**	**3. Design / Planning - 4, 12, 24, 31, 33, 44, 45, 47**	**4. Leadership - 7, 15, 22, 28**	**5. Training - 5, 14, 16, 17, 34a, 40**	**6. Policy - 18, 21, 25, 26, 27, 38, 39, 43**	**7. Culture / Communication - 19, 20, 23, 32, 34, 41**	**8. Procedure / Process - 2, 3, 9, 10, 11, 30, 35, 37, 39**
1. Requirements	X							
2. SETR - Lack of procedure								X
3. ICS/CDD								X
4. Keep malware off platform			X					
5. Resilience					X			
6. DoD demand for cybersecurity knowledge								
7. Organizations lack cybersecurity knowledge and manpower				X				
8. Unfunded cybersecurity mandates	X							
9. Many versions of Cyber/ Vulnerability risk Assessments (CRA/VRA)								X
10. Attestation								X
11. Logistics Cyber - Sustainable and usable by operator								X
12. Cybersecurity for partner nations	X		X					
13. Contracts - SOW/PWS - Budget								
14. PMs - Knowledge/Awareness					X			
15. Enforcement - Policy - ATO				X				
16. PMs - No Emphasis due to lack of previous programmed funding via FYDP / POM due to emergent requirement.- No Major Incident - Recognizable specific impact. Intelligence and STAR / VOLT inadequate yet to precipitate required programming.					X			
17. Certifications - Not enforced / affordable					X			
18. RMF - Always behind the adversary- Needs PM leadership						X		
19. Cybersecurity analogous to Safety- High Cost /No upfront ROI							X	
20. Requirements Exist - Not understood or enforced							X	
21. RMF not new for SIGINT						X		
22. Authorizing Official (AO) - by type system				X				
23. Cyber needs PM relevant language							X	
24. SE vs. Cyber Trade-offs			X					
25. Not Statutory - Too many waivers						X		
26. Boundary definitions – System of Systems						X		
27. Too many accreditation packages - Need Strategy						X		
28. ATO vice real security				X				
29. No Real Foundation of Requirements- No traceability	X							
30. Poor Rigor/Process for SSE- No relevant courses for embedded / weapon systems								X
31. Cybersecurity is thought to equal Business Systems- Not considered in weapon system design- No applicable to embedded systems			X					
32. Performance Based vs. Checklist Compliance							X	
33. Contractor Security			X					
34. Knowledge/Classification Gap							X	
34a. Ethical Hacking (must be taught)					X			
35. Must show remediation								X
36. Must develop solutions - Not COTS								
37. Intelligence is inadequate – RFIs are required								X
38. No effective SSE process/framework						X		
39. NIST 800-160 - System Security Engineering for Cyber- Esoteric concepts, Not useable						X		X
40. Push Training Left (CALIT)- CTT/CRA up front- Need Platform Acquisition Cyber Knowledge					X			
41. Messaging (culture) -Directive, Assistance							X	
42. Emergent Threat- Programmatic Inertia		X						
43. INFOCON not aligned with weapons						X		
44. RF is Issue (wireless!)			X					
45. Need Security controls for Real Time Operating Systems (RTOS)			X					
46. Foundation vs Ad hoc- Balance: Agile		X						
47. Legacy System Approach			X					

Figure 5: Data Reduction Heat Map

10 Conclusion

The experiment performed was a successful attempt to explore the technical through cultural issues that arise when trying to consider the impacts and safeguards of cybersecurity during the acquisition/life cycle management process. The information derived from this experience will be used to further refine the DAU curriculum to enable the acquisition workforce to better develop and maintain resilient/survivable warfighting capabilities for both now and in the future.

However, the exploration is never truly finished. Further experiments are being planned to continue to dial-in curriculum gaps as well as to explore similar cybersecurity issues during operations. We highly encourage to digest and to comment on what you see here on our attached forum discussion board in order to spark further discussion that can lead to real action and success.

Appendix A: Main Initial Concerns

Table 1A: Main Initial Concerns by Individual

Item	Concern
1	How to implement the mandates in the National Defense Authorization Act (NDAA), specifically Section 1647 requiring to identify and mitigate platform information technology (PIT) [also called embedded system] vulnerabilities. Some of these, like the avionics portions, are currently being evaluated and trained, but others lack resources to fully implement.
2	What affects the DoD in terms of cybersecurity issues in aircraft will eventually affect our partners that we are working with as well as participating in foreign military sales with.
3	Trying to bring together the programming, contracting and budgeting together in order to ensure that the technology requirements are built into the contract requirements to ensure the required capabilities. Concerned that the acquired/developed product is ready for deployment by being suitable, effective, and sustainable for when it's given to the fleet it does what it is supposed to do when it is supposed to do it. Also ensuring that it doesn't end up "auguring into the dirt" because there are more advanced weapons systems and/or more vulnerable to cyber threats.
4	Most PMs understand that there is a cybersecurity thing they must do at some point in their program, perhaps some system survivability key performance parameter (KPP), etc. However, it is only something they worry about when it comes to their milestone review. PMs are still not addressing that until it's too late and then they have to find resources to take care of this ad hoc. "… until the folks in the E-Ring start holding us more accountable in things like ADMs and milestone review, I don't think that it will get any better. One of the ways to do that is to design it better. To think about this early, I mean, we say that all the time. Well, we have to think about this stuff up front and often, but what are we really doing to enforce that? We don't do it.
5	On the current PM, level 2 curriculum, there are few cybersecurity teaching points. "In there we spend about 5-minutes on it and that's it. And the level 3 gets a little bit better. You are supposed to design some cyber into one of the early exercises, but we give it some attention, but that is about it. A lot of it has to do with time. If you are going to spend more time on it [cybersecurity] we got to take something out of the curriculum." Acquisition professionals need education and guidance earlier on that can help them navigate the process instead of just working the process as they go.
6	When asked the reason for lower enforcement of cybersecurity, "…there hasn't been a major incident like someone hacking a Tomahawk Missile and hitting a Mosque instead of the target."
7	Also on the lower enforcement issue, of cybersecurity, until the funding people, at the Pentagon, start putting money towards it, it won't have the proper employee incentives in their performance reports to drive these activities, not to mention it could be illegal to spend money on it in the first place.

Item	Concern
8	Fraud, waste abuse. No enforcing the standards because it's not affordable. Continue to throw people at it, and when they are not suited for it, they are leaving. Also "…the training piece is radically unaffordable." "Then you have the RMF monster in the room." DoD seems to change their standards every week. Also, for all systems, connected or not, you need an accreditation. To get that on a Navy network it must meet NETWARCOM's requirements as handed down from 10th Fleet using an RMF process (not sure why it is just not straight from DODIN requirements). Changes seem to be occurring so rapidly in RMF that if a small business wants to build a weapon system it is a major barrier to producing a solution because they will have to spend many resources hiring experts on the process to meet requirements that seem to be changing at least monthly. Also concerned about PMs not running their teams more like a Captain on a ship to ensure more "skin in the game." Focus on training to help the PMs get the folks with the skills they need (e.g. Security+ class, etc.). Also concerned with influences of money getting in the way of developing security/capability. Programs are driven towards programs that provide more money and capability, but meanwhile IA/cybersecurity is usually a money spender/resource taker with uncertain results and may sacrifice capability which makes it an uphill battle.
9	In reference to a 2006 NIST 800-53 manual showing RMF structures have been around for years, but the problem is, "we are not following it [i.e. RMF]." "…when you talk about the fleet defining requirements up front, what's the first things that define what protection level (PL) are you going to build to, or what mission assurance category (MAC) level you are going to build to; you're defining the user population and your levels of concern [Confidentiality, Integrity, Availability]. How often have you seen in a capability development document (CDD) where that's defined for you, so that you know what level you are going to be building this to? Rarely does that occur." "Those basic concepts, the levels of concern for integrity, security, availability; those things need to be defined up front, so that you as a program manager, you then can go, 'ok, I need to build this to a protection level four, because I have this user population that is going to be using the equipment.'" Another is that there are two accreditation pathways, DCIDs [intelligence community physical security standards for sensitive compartmented information facilities]. Also concerned that some don't understand the concept of accrediting authority which actually depends on what systems you are deploying. For example, if you have a SIGINT [Signals Intelligence] system, by statute, NSA [National Security Agency] accredits those systems. It is also possible that you may have to have multiple accreditation packages to deal with. "The other thing … to get across is, you know, you mentioned safety; this is nothing more than an 'lity', if you will, you know, maintainability, reliability, which are measures of quality. Well, cybersecurity is the same thing. It's a measure of how good your security is and it should be treated the same way in that regard."
10	There is also a concern that, due to culture or other factors, program leads are not bringing in cybersecurity members during the acquisition process such as voting boards as required.
11	Working both information and physical security together can be appreciated because it provides the perspective similar to a program manager in terms of bringing together cost, schedule and performance. If you can relate it to them in that regard that would really help when looking at tradeoffs with all of these inherited controls. I can see that,

Item	Concern
	"Hey, I could save time by doing this if I use this inherited control here or vice versa." This should be taught to PMs as well.
12	The security boundaries are a concern: Doing DICAP is not a strategy. "A strategy is how many accreditation packages you have, where you draw those boundaries, who's going to accredit, what interfaces you have with other interconnected security agreements that you are going to have to establish." There's an example of a UAV program with over 46 packages in it. If you don't understand that and get a strategy for all of those packages, it could result in a lot of costs.
13	Too much focus on "give me an ATO [Authority to Operate]" and not the spirit to provide security to the system. Hard to trace back to requirements because the requirements were not well established. "…I've looked at a lot of programs, doing risk assessments and different functions, [there] is very poor rigor in terms of system security engineering at the moment. There is no solid process, and you start tracing everything back to every regulation, every policy, and say, 'Yeah, great it's all regulation and policy, but you go back and, what kind of process is there, and everybody points to the "System Journey-B" model and not everybody does "System Journey-B" the same. So, you start looking at people that are doing systems engineering functions, and, yeah, they are good engineers, but have they had any cyber education at the entry level? No, because it was before their time. So, universities and academia are just starting now to sort of think about cyber in their curriculum and it started off as, 'Here's some networking course. Here's some very basic things, but there was no true engineering, or embedded systems engineering for cyber at all. So, we got another twist on it in that we have embedded systems, so policy and all solutions point fingers toward, 'Hey, its enterprise, we could use all of this different stuff.' Yeah, no, we have an embedded system running on a real-time operating system, so all of your solutions don't work. So, everything has to be unique and try to convince programs to go down that road is a hard sell."
14	What we're doing in NDAA 1647 to provide intelligence assessments to understand the threats so they can be prioritized and measured for success? Interface with the Fleet has been key for requirements flow.
15	NIST 800-160 in terms of its overlap with 800-54 and attempts at secure systems engineering guidance is too high level in order to provide practical guidance.
16	Requirements and related "unfunded mandates." "Cybersecurity needs to be done and … you have to get it out of hide because I've got no money for you. So, how do you deal with that?" This drives PMs to not only just to "get the ATO," but to only start thinking about it when the ATO starts to get addressed. There needs to be a way to incentivize thinking about and implementing cybersecurity from the beginning ("pushing to the left"). Cybersecurity also has to be considered for the entire acquisition cycle, even in the grave because there may be parts of that system that could be used to exploit new and existing systems.
17	Recommend to take a look at, if you had to go to war right now, what do you have. From there, take look at current vulnerabilities both now and perhaps down the road. When you do that capabilities assessment, use this lens to develop requirements. This could be powerful with developing the requirements in the ICDs and CDDs. It's not unusual to just throw together something at the end to "get the ATO." The Platform Acquisition Cyber Knowledge (PACK) Book establishes cybersecurity requirements

Item	Concern
	during operational requirements development. If not this, at least "… some sort of enduring document that goes along with that acquisition program and then you would be able to say, "How well did I answer the cyber requirements that I put out there."
18	To counter "pushing things to the left, "…you can push things more and more to the left, but you are assuming more risk. 99% of NAVAIR programs are not pre-milestone A; they're mostly legacy. "There's a recognition, my program needs cybersecurity, how do I get that, and by legacy, I mean JSF and everything back." "So, whatever solution you come up with has to be retro-fittable back to whatever's currently deployed." There needs to be a way that cybersecurity requirements are looked at as well. Had contractors in the past, say "here's what you do to support my process...[or]…to help me" However, PMs don't have to do anything, especially if it is put in a context of others that don't drive the boat. A good messaging approach would be like, "here's something the regulations say you have to do, I'm here to help you get it done at the minimal cost, minimal schedule, and here's the tools I have to offer you."
19	Program Management Guidebook, particularly for the RMFs, the reason why the document is not as successful is because they didn't do what we are doing here (i.e. a workshop to discuss cybersecurity issues vs. production.
20	"Whenever you say, 'cybersecurity' I guarantee you, 99.9% of the time they are going to think IT Enterprise. They are not thinking weapons, control systems, platforms. A study was done previously and it showed the impact of cybersecurity not being considered in developing a platform because the test involved essentially trying to look at the platform from the vulnerability perspective and there were many vulnerabilities found.
21	On the other side of the coin, there are situations where IA/RMF is followed too strictly which doesn't help the overall system function. "A prime example was finally winning the yearlong argument of why you don't need a CAC in an aircraft. Or even logging into any other weapon system. If we don't know what to do with a weapon system we default to the RMF structure, etc.– The CAC issue also exists with … Portable Electronic Maintenance Aids (PEMAs). "If I'm worried about somebody getting to my plane where I have to install a CAC card reader, I've got bigger problems on my flightline." This comes to the idea of "Performance-based cybersecurity" … "is essentially testing and evaluation (T&E), cyber T&E, penetration testing to test your system to see what flaws are in there." First, verifying known vulnerabilities and potentially finding unknown vulnerabilities or 'Unknown functionalities' of your system, because when you, "start throwing 'trons,' 1's and 0's, or other data/malformed datasets into a piece of gear, that's going to do something that you are totally unplanned for because no one ever thought about it."
22	"There's just a general knowledge gap part that we struggle with filling." There is not a good unclassified way to walk through how to hack through planes and ships. This makes the program offices "guess in the wind" or using IT approaches. However, it goes back to showing that the default look at cybersecurity is from an IT Enterprise perspective, and they figure if their system doesn't have an Ethernet port then they don't have any issues. Also, this keeps them from engaging the intelligence community to help understand threats to look at countering. "Because they don't have that knowledge base, they are unable to go to intel and ask the right questions." "If you ask intel, you know, 'What are the cyber vulnerabilities on 'x?' Unless 'x' is a very, very

Item	Concern
	specific thing, they will come back with nothing because that's not how they work….and so you don't get intel, since you don't get intel you don't get requirements, because you don't get requirements, you don't get funding and so the thing around us is that it all comes back to is a general lack of core knowledge of what it is that we do. And so, what we end up having to do with our tests is to take them [PMs] back to our lab… and basically walk them through the entire chain, 'Here's how we built these tools and why we built these tools; here is what we are exploiting with it.' And once we've walked them through that and get them onboard, it tends to get a lot better and a lot easier to work with them and they even start advocating their own, 'Hey I need money to fix this,' … But, you kind of have to walk them through it and give it the explanation of "this is what it really means to hack your platform."
23	This is where DAU could come in. It doesn't need to be classified. It just needs to be a non-IT Enterprise, where you don't have any TCP/IP network, (1553, etc.) and walk through "how do I hack it." "This is what your adversary is going to do to them…these are the steps…these are what it needs…and get them in that mindset, because once you prove that its real and give them the knowledge of "Here is what I'm looking for," "Here is where I'm going to get it." "Here is why I'm going to do it," then they tend to get on aboard very quickly. One example of educating PMs was in a navigation office. The office basically stated that their system was not subject to exploitation because it was too complex, etc., but once shown about five "GitHub" PH. D/other projects that showed how they reverse engineered and broke the system (all open source) they began to understand more of their ground truth. Otherwise, they just think this is a money sink that will probably change as new leadership rotates, etc.
24	One of the biggest complaints of this approach is that PMs feel that they are just going to "poke them in the eye" when red teams come in and find issues. Answer: This is where explaining the remediation is key. This can go the other way and go too far (CAC Card example) or its going to cost $200 Million. It is also important to understand nation state, hard to do hacks, versus an easy hack that can severely impact systems and take these into account in the RMF process. Bringing all points and perspectives together to get to the acceptable security needed. These teams not only have to find the vulnerabilities, but should work with the PMOs to design remediations that can meet power, weight, airworthiness requirements to fix them within an affordable budget.
25	On the subject of different INFOCONs and "silent running" ideas in relation to vulnerability, "These are built to target you when you are dark." These are not TCP/IP tools. You are mainly targeting your side channel bands, so you are not going in through your normal TCP/IP. These systems may be still on even if it looks like they are off. Your bus architecture can be a viable entry, etc. Basically, targeting the systems you trust. Muppets act as a tool kit for this purpose. Much more detail could be classified which creates another obstacle when it comes to educating acquisition members in this area.
26	We often don't know what questions to ask (referring to the unknown unknowns). And you don't always have red teams/vulnerability assessments in pre-milestone A. The first time they get to touch the system is when they start to test. To the A-10, they could build it to survive a "bullet" because that was very well defined prior to the A-10 development. "We don't know early on what the electronic profile of that aircraft is going to look like. We don't even consider it. EW or cyber can be equally difficult. We

Item	Concern
	think about that during test. Major programs such as the F-22 or F-35 can have a decade or two gap between developing and fielding and what do you do with that? “What’s the security control for an embedded system? We don’t know. Even if we do attack the problem back here we haven’t done the basic science or there’s not enough people attacking the basic science to go ahead and inform our decisions back here.” This is where there is a default back to Enterprise IT security that doesn’t meet PIT mission goals (i.e. CAC cards in weapons systems).
27	“There is no such thing as a simple fix.” - We need to understand/design the cybersecurity requirements early in the baseline. The cost of finding it in the sustainment phase, or even late in the acquisition cycle is very cost prohibitive. They would have to fund a study to determine vulnerabilities, and then have to develop a solution, on an unfunded requirement campaign, and try to get it on contract, integrated and certified (IA, Airworthiness, etc.) which can delay that part of the program, potentially, for years.

Appendix B: Day 2 Initial Findings Data Reduction and Prioritization

Day Two (18 May) Data Reduction:

Overall (Heat Map):

1. Requirements - 1, 8, 13, 29
2. Reaction/Resilience (Response) - 42, 46
3. Design/Planning - 4, 12, 24, 31, 33, 44, 45, 47
4. Leadership - 7, 15, 22, 28
5. Training - 5, 6, 14, 16, 17, 34a, 40
6. Policy - 18, 21, 25, 26, 27, 38, 39, 43
7. Culture/Communication - 19, 20, 23, 32, 34, 41
8. Procedure/Process: 2, 3, 9, 35/39, 37, 10, 11, 30

(Normalized Data Capture):

1. Requirements
2. SETR - Lack of procedure
3. ICS/CCD
4. Keep malware off platform
5. Resilience once it gets on
6. Hunger for info
7. AFRL - Not manned to fix
8. Unfunded mandate
9. Lots of CRA/VRAs
10. Attestation
11. Logistics Cyber - Sustainable usable by operator
12. CYBERSEC for Partners
13. Contracts - SOW/SPW - Budget
14. PMs - Act like 1st time heard cyber - Knowledge/Awareness
15. Enforcement - Policy - ATO
16. Education for PMs - 5 min

   a. No Emphasis - Due to lack of previous programmed funding via FYDP/POM due to emergent requirement.
   b. No Major Incident - Recognizable specific impact. Intelligence and STAR/VOLT inadequate yet to precipitate required programming.

17. Certs
    a. Not enforced
    b. Not affordable
18. RMF - Monster/Construction delta
    a. Always Behind
    b. PM leadership
19. IA/CYBERSECURITY like Safety
    a. Cost $
    b. No ROI
20. Requirements Exist - Not understood or enforced
21. RMF new? Not for SIGINT
22. AO - by type system
23. Cyber Needs PM Language
24. Trade-offs SE vs. Cyber
25. Not a Statue - Too many waivers
26. Boundary - SoS
27. Too many accreditation packages - Need Strategy
28. Just give me an ATO
29. No real foundation of requirements
    a. No traceability
30. Poor Rigor/Process for SSE
    a. No good course for embedded
31. CYBERSEC = Business Systems
    a. Not considered in design
    b. No applicable to embedded systems
32. Performance Based vs. Checklist
33. Contractor Security
34. Knowledge/Classification Gap
    a. @ Hacking (must teach)

35. Must show remediation
    a. Must develop solutions - Not COTS
36. Omitted
37. Intel - RFIs
38. No effective SSE process/framework
39. 800-160 - too high
    a. Esoteric concepts
40. Push Training Left
    a. CTT/CRA up front
    b. Pack - Requirement traceable (Platform Acquisition Cyber Knowledge)
41. Messaging (culture)
    a. Directive
    b. Assistance
42. Emergent Threat
    a. Programmatic Inertia
43. INFOCON not aligned with weapons
44. RF is Issue (wireless!)
45. Security controls for Real Time Operating Systems (RTOS)
46. Foundation vs Ad hoc
    a. Balance: Agile
47. Legacy System Approach (CBA)

Appendix C: Breakout Session #1 Question/Answer Details

Table 4A: Team 1 (Contracts/PMs) Q&As for Breakout Session 1

Team #1 (Contracts/PMs)	
Question 1	**What functionalities are actually needed?**
<u>Team #1 Answer</u>: "Cyber is not some sort of special competency here all their own, it's another part of engineering, it's another part of test." Also, as a PM, you need to know enough to know when requirements are not being met and a reasonable level of effort estimate to satisfy such requirements. Need to understand what you are buying on a contract.	
Question 2	**What is your role/responsibility in this area?**
<u>Team #1 Answer</u>: Taking what the resource sponsor brings down and coordinating it. Supporting the Analysis of Alternatives (AoA). Team Staffing – Make sure you have the funds in place to bring the right cyber support staff, engineers, etc. Must also consider the tradeoffs; examples being value added for cybersecurity vs. other system needs (engines, etc.).	
Question 3	**Who are the people that should also be engaged?**
<u>Team #1 Answer</u>: Basically, the whole integrated product team (IPT) needs to be brought in up front because if you are putting in cybersecurity requirements it's going to affect design, logistics, tasks, costs, even your contracts/budget folks; they need to understand what's going on there, and also the users in the Fleet. User representatives at NAVAIR, for example, are fresh from the fleet and may be able to offer an operational perspective to the acquisition process. Flight test and the development/test squadrons can do this as well.	
Question 4	**Where is it important to use cybersecurity experts?**
<u>Team #1 Answer</u>: Basically, everywhere. Specifically, specification development, where you are putting them on contract; you need them there. Supporting the cost for alternative analysis. For example, they may be able to act as advisors when contractors are presenting solutions and related cost/effectiveness for risk tradeoff and getting the best solutions for the cost. This can also be helpful especially during contract evaluation where understanding a level of effort can help to estimate the value added for the cost spent (a radical $5 Million for 5 hours work example was used to understand reasonable cost estimates).	
Question 5	**How could a compromise in systems "x" affect system "y"?**
<u>Team #1 Answer</u>: Basically, if you don't address your cyber considerations up front, you are going to pay for it later with cost and scheduling loss. Functionality risk analysis with the AoA, bottom line, saves time and money by coordinating the cybersecurity requirements as early as feasible, as many others may be affected.	
Question 6	**How does this affect RFP/SOW/Contracting wording?**
<u>Team #1 Answer</u>: Everything. If you don't have the right requirements, and understand the general level of effort of the tasks being purchased you may have to change it during contract execution which results in a lot of lost time and money.	
Question 7	**A lot of people are going to need to support you to get this task done, is there that much [cybersecurity] talent available out there?**
<u>Team #1 Answer</u>: Could be dependent on the size of the program/availability of funds.	

Team #1 (Contracts/PMs)	
Question 8	**If you had to cut 10% out of your budget for cybersecurity how would you do that?**
Team #1 Answer: Would ask our cyber folks to provide a prioritized list of tasks with the related impacts. Then present to the program manager(s), so they could look at a tradeoff with something with the aircraft. One example would be if there were an upgrade, etc. of the same cost that would add 10 knots of speed to the aircraft, it might be more important to address some cybersecurity issues in the engine instead to prevent a hostile shutdown, etc.	
Question 9	**Has anyone ever seen a prioritized list of cybersecurity requirements?**
Team #1 Answer: Yes, sometimes organized into Security Technical Implementation Guide (STIG) CAT 1, 2, 3. One way you can get there is through a cyber risk assessment. You have to engineer it, man it, and scope where the cybersecurity is needed to really determine their availability and expense, just like any other part of the program. Supportability/cyber maintainability is a key issue. If during the longer-term development as a weapon system, for example, the firmware is going to need upgrading throughout the that period, even in sustainment. Thinking about it and coordination between logistics and engineering early could result in an access port being designed in rather than having to take it apart to update the latest software to minimize overall increased delay and costs. Bringing different disciplines early can establish these requirements where they are more viable and sustainable.	
Question 10	**What are you, after you went through this, what's the thing you are most worried about in this stage [cyber domain Pre-Milestone B]?**
Team #1 Answer: "Having a good handle on my cyber-derived requirements…because once I have that I can figure out what funding I need, what schedule I need, what people I need, but if I don't have good requirements I've got no idea if I can even execute my program or not." Trained cybersecurity resources are often scarce. PMs must be aware of the fact that they may have limited access to a cyber SME, especially for smaller and/or legacy programs.	
Question 11	**Are there PEOs or Program Management Agreements (PMAs) involved in this?**
Team #1 Answer: PMAs are involved, otherwise they couldn't execute their programs.	
Question 12	**Can you act as program manager even if you haven't been officially designated?**
Team #1 Answer: Yes, there are engineers that can be qualified [with leadership designation]. There's some confusion over how things are run before they become a program of record vs. after they are an official program. You may not have had the official budget, but you've been a PM the whole time. "The main goal today is to try to enhance some of the curriculum to include, so in the PM stuff, why don't we start, instead of talking about cybersecurity as its own separate thing, right? Shouldn't we start thinking that these are requirements like any other requirement that I have now. So, these should be addressed early on in my requirements traceability matrix, when I do that engineering 'V' walkthrough and have my systems listed at the top my functions listed over here. Shouldn't we include cybersecurity stuff in there as well…?" On teaching level 2 students they tend to "…see cybersecurity as this thing of its own, off over here that they eventually have to worry about. I think if you want people to start thinking about it sooner or taking it more seriously, they should treat it like any other requirement. If your aircraft needs a radar that can go so many miles that's fine, that's one requirement. There might be another requirement underneath in the traceability matrix that will keep that secure from a cybersecurity standpoint."	

Table 4B: Team 2 (Test and Engineering) Q&As for Breakout Session 1

<table>
<tr><th colspan="2">Team #2 (Test and Engineering)</th></tr>
<tr><td><b>Question 1</b></td><td><b>What is your role/responsibility in this area?</b></td></tr>
<tr><td colspan="2"><b><u>Team #2 Answer</u>:</b> The team decided to look at functionalities from a CIA perspective.
<b>Confidentiality</b> - Unclassified to Secret, platform dependent. A lot of the manuals are usually unclassified, but the loads can go to Secret. Going to need some sort of multi-level security or PRH processing to provide protection. PRH allows to transfer information from one security level to another.
<b>Integrity</b> – People could be hurt and missions could be lost from the introduction of corrupted data.
<b>Availability</b> – (Medium) – User population would be the maintainers. A main concern is if the mission data is wrong whether by accident or design of a bad actor. While considering the user and the level of classification of that data, they considered user vetting for different classification as the information flows and/or “jumps” from the data sources to the equipment/weapon system being maintained. This can help to identify up front mitigation plans for a PEMA malfunction, compromise, etc. to minimize mission impact. Also, knowing the environment the equipment will be in, such as an aircraft carrier, could result in leveraging protections that are already in place, such as employee vetting, physical access security, etc. If necessary, the equipment being developed may result in additional vetting/physical access requirements (even exercises) for that area, which should be coordinated early.</td></tr>
<tr><td><b>Question 2</b></td><td><b>What functions/roles are actually needed?</b></td></tr>
<tr><td colspan="2"><b><u>Team #2 Answer</u>:</b> In considering the different roles of this exercise, coming from a test and engineering perspective, the team considered risk assessments and characterizing the attack surface, as well as helping with threat intel from previous experiences. Specifications refinement can be key to minimizing to only needed software and applications (for instance, if the web browser or other applications are not needed, they can be removed) to lower the overall vulnerability footprint, etc.</td></tr>
<tr><td><b>Question 3</b></td><td><b>Who are the people you that should also be engaged?</b></td></tr>
<tr><td colspan="2"><b><u>Team #2 Answer</u>:</b> This is also a good time to engage with the system architects, subject matter experts (SMEs) as well as, and Cyber Safe (mission assurance based on Sub Safe program, only for Cyber) RMF personnel to start to figure out the controls they should use. On the Principle Crediting Authority, the challenge would be to engage them early as it appears by some accounts that they currently don’t want to engage until you have the system almost completely designed; because it could be in their job queue for years as development continues. Incentives are needed for the accrediting authorities to engage earlier and not be penalized for long times in the queue. One possible solution is to split the process into two parts that the authorities could accomplish at both ends. That way it shows completion of each while engaging earlier in the process. Early data owner engagement is also key because they will ultimately decide what controls and levels of security will be required.</td></tr>
<tr><td><b>Question 4</b></td><td><b>Where is it important to use cybersecurity experts?</b></td></tr>
<tr><td colspan="2"><b><u>Team #2 Answer</u>:</b> The answer is throughout the life cycle process, however, because cyber is less quantifiable (can’t just measure and store like physical wing parameters), as well as more dynamic, so these experts will need to consult as the lifecycle progresses to ensure mission success.</td></tr>
</table>

<table>
<tr><th colspan="2">Team #2 (Test and Engineering)</th></tr>
<tr><td><b>Question 5</b></td><td><b>How could a compromise in system “x” affect system “y” [interdependencies]?</b></td></tr>
<tr><td colspan="2"><b>Team #2 Answer</b>: Because you are loading the Operational Flight Program (OFP) and other info to the systems, any compromise to this information could result in direct effects to the mission. Subjects of little data validation at this level, many people involved in the handling, as well as wide effects/attack foot print considerations were discussed. Also, if specific needs to fix things (cybersecurity) are discovered, it could be very difficult to find time and funds to correct. That is why early involvement is so critical.</td></tr>
<tr><td><b>Question 6</b></td><td><b>How does this affect Request for Proposal (RFP)/SOW/Contract wording?</b></td></tr>
<tr><td colspan="2"><b>Team #2 Answer</b>: It is very important to come to a consensus of, and then get buy-in from, the stakeholders, to include the contractor(s), to ensure clear language that will satisfy those needs. Also knowing what classification was required allows for proper DD Form 254 documentation early. The goal should be to aim for about 99% of the issues, artifacts, and controls being identified early to minimize exponentially rising costs to fix later in the cycle. Recent examples discussed were more like 80%, but the key was to team together to identify requirements early in the acquisition process for best likelihood of success.</td></tr>
</table>

Table 4C: Team 3 (Logistics) Q&As for Breakout Session 1

<table>
<tr><th colspan="2">Team #3 (Logistics)</th></tr>
<tr><td><b>Question 1</b></td><td><b>What is your role/responsibility in this area?</b></td></tr>
<tr><td colspan="2"><b>Team #3 Answer</b>: The logistician’s main goal is to, “Influence the system design by bringing his/her knowledge about sustaining and maintaining a system into the equation as the engineers develop it. It’s also where we start to develop a lifecycle sustainment plan. Very vague at this initial stage, but as the process gets closer to the PDR, the sustainment plan will start to mature and fill in the various ‘IPS’ [Integrated Product Support] elements (e.g., how do you man it?; How do you train it?; What other requirements?) The main idea is to remain relevant and vocal during a system development to make sure it’s sustainable once fielded.

One of the discussion topics was the concept of ‘Contractor Logistics Support (CLS)’ vs. organic logistics capabilities. That will become a very important factor based on the potential cost increase associated with CLS. But, if you go organic, will you have the cyber experts to maintain something like this? For example, “The day when Boeing decides they don’t want to maintain software for the A-3D variant anymore.”</td></tr>
<tr><td><b>Question 2</b></td><td><b>What about PBL [Performance-Based Logistics]?</b></td></tr>
<tr><td colspan="2"><b>Team #3 Answer</b>: We are all supposed to switch over to ‘Performance-Based Logistics’ now? Not to be confused with CLS?” How do you factor cyber into a PBL strategy?   “If you add in CLS also having to worry about the cyber perspective; their networks; their databases; how they connect to components that they are repairing at their facility.” If we have a component that we decide through the various metrics and studies performed that we, for example, pull the brakes from the aircraft and send it to the contractor for repair because that was the cost decision of the program manager, from a cybersecurity perspective, what do their benches look like? Do we levy that in the contract? These decisions come and things go down the acquisition life cycle. These are things that play into the maintenance plan of your system, so if we’re levying additional cybersecurity requirements that are funded, as a logistician, I have to be mindful of that and lean on my cybersecurity experts to keep me honest when we start writing contracts, RFPs, SOWs, etc.</td></tr>
</table>

<table>
<tr><th colspan="2">Team #3 (Logistics)</th></tr>
<tr><td><b>Question 3</b></td><td><b>What happens when things become obsolete? Are these planned into the ACQ lifecycle?</b></td></tr>
<tr><td colspan="2"><b><u>Team #3 Answer</u>:</b> As vendors move to new technologies, it costs more and more to maintain the older technologies. Examples of this are where an ‘ICS’ that was cost prohibitive because only one contractor could maintain it and also a ship’s IT systems being very outdated because the IT contract was let 10 years before the ship was actually delivered. The Navy later included “design envelope” options that would allow them to put in whatever they needed up to a year or so prior which cut this problem by about 80%.</td></tr>
<tr><td><b>Question 4</b></td><td><b>“If I can do something to your data, do you care about that? Even in a gradual manner such as changing the number of engine cycles to increase engine changes. Is anyone worried about that?</b></td></tr>
<tr><td colspan="2"><b><u>Team #3 Answer</u>:</b> I don’t believe that they would look to the PEMA, but would go to the engine contractor and start asking why the engines seem to be changing out so soon, but you are right that people might not see this.
We are thinking about how to build, maintain, and dispose, but are not thinking about the data that drives these factors. “It’s just a way of thinking.” We now have to look at how a hacker thinks, so we can do these things better.
“The main question is: Whose responsibility is it for ensuring cybersecurity is adhered to?” “Does the cybersecurity person that’s hired answer to the Assistant Program Manager for Logistics (APML)?” If the answer is ‘Yes,’ then it’s a logistics function. Does that person answer to the systems engineer? If that answer is ‘Yes,’ then it’s a systems engineering function similar to configuration management….”
“I don’t think it’s either one, I think it’s the principle accrediting authority. If something bad on the system happens from a security perspective who do they go after? They go after SSO Navy. “Hey, how come you didn’t protect this data, that SIGINT data, that you were charged with?”
However, it’s not just who do we go after, it’s who’s going to protect it? Logistics have been used in the past to bleed out enemies in terms of time and resources. What if we design ways to detect these bleed outs during the acquisition process? For example, having data analytics to show that when we are in this port, certain functionalities, etc. fail 40-50% more. Ensuring someone is looking at that will allow the threat to be identified and countered. It’s good that we are talking about having cybersecurity experts in the IPTs, but what about training some PMs, engineers, contracting folks in cyber?</td></tr>
<tr><td><b>Question 5</b></td><td><b>What is your worst worry given the cyber scenario?</b></td></tr>
<tr><td colspan="2"><b><u>Team #3 Answer</u>:</b> “It’s more of the unknown unknown. What could be a big loss is if we had to move things up a level of classification to protect the system. Barring that, if we have to run on an unclassified system, that we know is probably compromised in some way, how do we assure the integrity of the information on that system and it is operating as it supposed to? There is a quality assurance process to help with integrity issues. “I’m an executer, so how do we functionally take the cyber stuff and apply it to our processes, so that we can safely field a weapon system?</td></tr>
</table>

Appendix D: Post Breakout Session #1 Discussion Details

Table 5A: Post Breakout Session #1 Discussion Details

Group Discussion After Breakout Session #1 Briefings	
Question 1	**Now that you have heard all the discussion what are your comments?**
All Group Answer: The Requirements are definitely a popular answer. Documentation is another important topic that can be punishing if not properly prepared from the start "So, being able to have access to your interface control documents, being able to view the software information instead of being stuck to just black box binaries; those are the important items to get involved with now as you know you are still early on in the program and make sure your contractor allows those. For example, [contractor] who is currently performing testing, has several RF systems that are still very early in the development cycle, but requested the contracting office approve them with the argument, 'Because these are so early on, any issue that's identified can be corrected before going to Fleet; so, there's not that big a deal, it's still in its normal software development cycle and they do a normal development requirements (DR). It was a good idea. We went there. We did the test. We got the results, and provided them to the contractor. Everybody was happy. However, the contractor is running into an issue when attempting to fix the identified flaws because they don't have the documentation rights for the systems. So, this whole workaround has required the original developer to get involved since the testing contractor does not have access to the source documentation/code. **Other examples** - One program, no ICD, no components on the platform, and another where they buy an entire platform as a black box and ask us to do testing on it, so we didn't even have a list of what's inside, how it talks, etc. Traditionally, not having access to documentation, such as the source code, made sense and saved money, but now this is needed to both identify and fix cybersecurity issues or at least access to the contractors that wrote it. Early on in the development you need those documents for reference as stated above. This should be included in the contract/other requirements. Must be some convincing that [perhaps using the recent changes in logistics as an example] to show how we can do this early in the cycle to save long term costs and hopefully to prevent a major incident before it occurs. We have this systems engineering, cyber systems engineering core of people [we are doing according to the group] How strong is it? Maybe not very much. There's the CIO accreditation person and the system engineer. Two different animals, aren't they? It is breaking to a certain degree at NAVAIR....We are moving away from a CIO driven cybersecurity to more of an engineering driven cybersecurity. Not as fast as some would like. When would you have certifications for core folks? SECNAV 5239.20 is trying to define what education and training (8570, etc.), but not to a certification like this yet. Because of the nature of IP, etc., It makes more sense to take someone from the Avionics and make them a cyber person than to take a cyber person and make them an avionics person. It has worked both ways. How would the certification work? As you analyze the required info path you start to favor one over the other. Especially during this development phase, shunning off anyone because they don't have a certain degree or certification may do more harm than good.	

Group Discussion After Breakout Session #1 Briefings

Question 2 | **How do you know who are the right people?**
Where do we go to get cyber help?

<u>All Group Answer</u>: What some have done in standing up the “114”…Cyber Secure was part of that.... When I say secure systems engineering, I’m not talking about just cyber, I have to consider other program protections including pen testing, etc. The minimum requirement will be at the 200 level, some groups are going to be at a 300 level, plus other courses that seem suitable, to start. So, that’s the 114. We’ve got 45, you’re doing the cyber, that’s great, we’ve got 5, 411, etc. “What I’m trying to do is to establish a…cross-competency systems security engineering (SSE) integrated test team (ITT).” Do we need to have a cyber kind of expertise in part of 45? Absolutely! T&E? Absolutely! Should also add in integrated logistics support (ILS)/PM. To show how to manage the requirements across the competencies. “Is there going to be one place to go to? I don’t think there should be.”

Question 3 | **How does it work in the Air Force?**

<u>All Group Answer</u>: We have an office within AFMC called “The Crows” Cyber Resiliency Office for Weapons Systems (CROWS). It is currently centered up at Hanscom with a lot of Wright Pat connections as well. They have a couple of SESs running where they are trying to figure out overall, across the Air Force, how are we going to handle this? Also discussed how they are working with intelligence organizations such as the National Air and Space Intelligence Center (NASIC) to be able to help them know what to go look for and that relationship has improved intelligence coming back overall. I’m seeing more and more contractor involvement because it is getting harder to train folks late in their career, so they are hiring folks that are getting out of the services or other places and you bring them along, and so, we are seeing a lot of that. For example, in my T&E community it seems that everyone we are talking to is a contractor.

Talking about core competencies (career fields) versus position expertise needs (avionics cyber, etc.). Talked about experiences working with Intel Officer Career Field Managers and how much cyber training/education do they need. (i.e. make an intel person a cyber person or make a cyber person an intel person, or both).

On the Total Force and their role in resiliency, the Government also has to compete with industry for this talent and industry pays more and can often hire faster, so it may come down to the Government leveraging industry to fill the gaps, hire at these speeds that we are not able to as Government. Defense contractors often have to compete with civilian contractors for the talent as well. Have we lost some trained Government folks? The group could name at least two, others didn’t know specific numbers, but confirmed that they had lost some too.

The Government usually has to deal with attrition issues as with other things, but normally, commercial industry understands what they are doing and the Government can sort of follow along, but with cyber, the civilian community is just as clueless as the Government, therefore, any person that bubbles up as being “good” is pulled from all directions.

Question 4 | **This makes for an interesting challenge for DAU, I would imagine, because who are you educating?**

<u>All Group Answer</u>: It’s all about recapitalization. Taking people that were already on a path and giving them help as well as new people that are coming in, but there is such a small number now. There is certainly a lot of people with a lot of knowledge and if you can just get them going in the right direction….

Appendix E: **Breakout Session #2 Question/Answer Details**

Table 6A: Team 1 (PEMA) Q&As for Breakout Session 2

Team #1 (Post Milestone B, Pre-Milestone C Focus)	
Question 1	**What functionalities are actually needed?**
Team #1 Answer: We have to freeze the baseline at 'critical design review (CDR).' This is to prevent scope creep, etc. Other changes can be made later during LRIP, spiral, etc.	
Question 2	**Who are the people that should be engaged?**
Team #1 Answer: The PM and the operator test (OT). Didn't have OT as of yet. No one includes legal and I don't know why. You can't get the Contracting Officer (KO) to do anything unless legal tells them.	
Question 3	**Where is it important to use cybersecurity experts?**
Team #1 Answer: It goes across all disciplines. Everyone needs to get trained in cyber or else they can't do their job anymore in the field that we are in. They don't have to be deep tech experts all of the time, but when the lawyer provides counsel, they have enough cyber knowledge to put it into the proper context. This applies to the KO and others in the same manner.	
Question 4	**Who could a compromise in system "x" affect "y" (interdependencies)?**
Team #1 Answer: Using the PMR on an airborne mission computer for example, if the mission computer was compromised then the aircraft could potentially crash. There was also an example of a mission computer onboard a ship that had to be replaced because it had three unsuccessful logins and the mission is affected.	
Question 5	**How does this affect RFP/SOW/Contract wording?**
Team #1 Answer: For engineering, tasks, Defense Technology Objectives (DTO), logistics, and all of your inputs for performance specification. If your specification is written correctly, and passes the specification into LRIP, the contract will be successful. The problem is that all tend to use Statement of Work (SOW), Statement of Objective (SOO), and Performance Work Statements (PWS) all the same when they are, in fact, different. The SOW is a design document [very specific design to tell the contractor how to build the product]. - Others disagreed with this statement, stating, the specification is the design document. The SOW (as included in the contract) is the vehicle used to direct the contractor on how to design, build, test, and support the product, as required. Conversely, a PWS will tell the contractor what is required, but not how to build it. - The requirements have to include input from everybody. They have to be very well defined, and that will simplify the task of writing a contract. As long as there is input from the engineering, the task, the logistics staff, it should be fairly easy to generate a PWS. - Others disagreed with this statement. "If it is simple, why does it take so long and require so much review and approval at such high levels. The Federal Acquisition Regulation (FAR) statute and other processes require many actions. A good requirement helps, but how often do we have a 'good' requirement." Also, the comptroller, legal, etc. are needed to ensure the right type of funds are being used, as well as all of the other technical specifications. It definitely has to be worded correctly. You	

Team #1 (Post Milestone B, Pre-Milestone C Focus)	
need contracts, comptroller, legal to ensure best success. Have to get the formal requirement to meet the technical specifications. Lastly, "If you have a contract that is ambiguous, the Government will lose every time." Provided an example of MI-17s when running an NVG lab. The contract only stated "endless" radiance. Using the word compatible vs. compliant allowed them to produce a product that made the cockpit too bright when using NVGs. They couldn't do anything about it because of the way the contract was ambiguously written.	
Question 6	**What if you were to say in specific or as general as you could be say, "The airborne mission control computer must be able to survive a zero-day attack?"**
Team #1 Answer: Most said it's too ambiguous because of the lack of definition of "zero-day" and "survive." Definitely need to provide [students] more examples of good and bad because there is not much out there.	

Table 6B: Team 2 Q&As for Breakout Session 2

Team #2 (Post Milestone B, Pre-Milestone C Focus)	
Question 1	**What functionalities are actually needed?**
Team #2 Answer: Cyber functionality is needed, but must be reevaluated at this point. In the later stages of development, it is very important to review and refine/update the current requirements and risks to account for any new information and artifacts in preparation for Milestone C. This review must also consider if the program is funded to meet the new and/or emerging requirements. It is also important to ensure that you are ready to meet testing requirements to avoid additional time and funding costs of delays. It is prudent to start looking at RMF controls and evaluation at this stage.	
Question 2	**What is your role/responsibility in this area?** **Who are the people that should also be engaged?**
Team #2 Answer: This is a good time to bring in the Operational Testers (OTs) to coordinate OT/development test (DT) activities and test on the actual equipment (i.e., not a simulator, etc.). Ensure that the maintenance and sustainability have been dialed in/sync'd. Check for interoperability with your operational test agency (OTA), product support, etc. bringing together what you had in Milestone B, updating it, refining everything, identify any additional roles and responsibilities, to include placing the right cyber people in the right spots.	
Question 3	**Where is it important to use cybersecurity experts?**
Team #2 Answer: "Everywhere. The team could not identify a stage of the process that doesn't need some form of cyber expertise or knowledge."	
Question 4	**How could a compromise in system "x" affect "y"?**
Team #2 Answer: You could think as broad as you like or in a minute be done, but our focus was on, being the scenario is a PEMA, we looked at the vulnerability of unnecessary software on the computer that could be running malicious code disguised as normal function and exfiltrating data. Software minimization is key.	

Team #2 (Post Milestone B, Pre-Milestone C Focus)	
Question 5	**How does this affect RFP/SOW/Contract wording?**
Team #2 Answer: By this time in the Milestone you should already be on contract, so hopefully changes in your documents and things you've discovered doesn't really change your "spec" much, but if so, to evaluate and to make the best decision to change any language based on need and to pass OT. Discussed the use of "orange" instrumentation, or out-of-band monitoring, to avoid blocking of monitoring, as well as avoiding memory/resource overloads of the systems themselves. Some efforts are being worked, but in order to consider on for your program it would have to be considered early and thoughtfully prior to test. "Driving the "orange" gear, the instrumentation [sensors] gear could be a big deal." Also, consider the existence of resources such as the cyber range to help with testing, etc. Also, considerations of where to put this documentation (Cyber Table Top (CTT) or cyber risk assessment (CRA)), especially when you are dealing with Joint programs where each service may do it a little differently. Also, with system formats such as a 1553 bus you may not know enough of what is supposed to be passed to detect issues. This is a key difference between TCP/IP and more PIT oriented formats as it is more difficult to understand what is happening or if a problem even exists (e.g. no "packet capture" software for PIT like Wireshark does for TCP/IP). This also is an issue for demodulating/parsing RF based signals given all of the different formats as well.	
Question 6	**Has there ever been a requirement of that kind for instrumentation on any platform?**
All Groups Answer: General consensus is no. But, feel it may be missing. This is akin to not having instrumentation on aircraft engines. With cyber, it seems the first indication is that the screen/functionality locks up. You may have to write up several requirements to implement this. Also, this brings up the tradeoff between anti-tamper and cybersecurity testing (i.e. access to serial ports, etc. to understand data flow). Anti-Tamper is supposed to prevent system compromise if the equipment falls into the wrong hands by making it difficult to reverse engineer. This has never really been a discussion until now, but if cyber instrumentation is installed to understand what is going on in the PIT system, this would make it easier for an adversary to defeat anti-tamper efforts. This could spark new discussion to understand these tradeoffs and make the best decisions. Compromises discussed included providing more access to serial ports for prototypes testing and then maybe more securing the production versions, etc.	

Table 6C: Team 3 Q&As for Breakout Session 2

Team #3 (Post Milestone B, Pre-Milestone C Focus)	
Question 1	**Why you were putting in reports for the first question (functionalities needed)?**
Team #3 Answer: One of the requirements to get out of the phase was to get your ATO. The verification of the CTT and CRA is key.	
Question 2	**From all that people have said, is there anything different from your users, people involved, etc.?**
Team #3 Answer: You may want to review you Plan of Actions and Milestones (POAM) issues that you want to fix later as well as try to get money for them. On RFP/SOW wording, when it comes to your contract changes, review agreements you have for your ITT and ATO.	

Team #3 (Post Milestone B, Pre-Milestone C Focus)	
What you need to do may require a change in contract in order to meet requirements. Also, applies to data/equipment accesses.	
Question 3	**I know we want cyber people everywhere, but how could we put a convention on it in terms of "what's good enough"?**
Team #3 Answer: It depends. "You have to look at what system you have, what threat environment it is going into, what you can afford, and what other risks you have to balance out in your program." Perhaps you could lay out some key questions to ask or guidelines to follow in this stage that might be helpful. By looking ahead, a year, and you realize that you will have x number of cyber-related tasks, ensuring that you have the right cyber people to cover it or at least put the request in. It comes back to asking the question, "What's going on in your program and what kind of support are you going to need to support those efforts in the program?" It will depend on the requirements as well as the type (CLS vs. PBL) to properly plan for resources.	
Question 4	**"What's your most important issue here?" What's the key thing or "showstopper?"**
Team #3 Answer: I would say the DMB and CRA where you know what you are getting done and that will feed into your plan of action (POA).	

Appendix F: Hot Wash (After Action Report) Details

Table 7A: Hot Wash (After Action Report) Details

Item	Concern
1	"Well, coming in here cold, I learned a significant amount of information about cybersecurity, that I mean, it was just non-existent, really except in a little caveat in some of the DAU courses I attended, so it was really eye-opening. One recommendation; I'm harping on this core competency type of thing, whose job is it; if we can't do that possibly filter it out to all of the disciplines, for instance, if we made an additional IPS element for the "loggies," a thirteenth one, maybe a cybersecurity IPS like the training and the manpower they have LEMs - Logistic Element Mangers, specific to those particular fields that might be one area to increase the knowledge. Could do the same thing for the other disciplines as well. Maybe not necessarily the PM because that's all encompassing, but definitely for the systems engineers. That may be one way to crack the nut to get this integrated as quickly as possible."
2	It was interesting and you [DAU] have a really important function here in trying to get together training for everybody. I'd like to invite you all out to Wright Pat at some point to get out to see what we are doing at AFIT. We have a whole division that is devoted to training in the Human Effectiveness Directorate and part of what they are taking on is cybersecurity, so it might be good to see what they are doing as well.
3	While CTT exercises may be helpful, they should not be mistaken or substitute for a Cyber Vulnerability Assessment (CVA). CTTs have the potential to discover some problems quickly, however they lack the systemic rigor and accuracy of a CVA. A properly done CVA should identify the entire range of potential cyber vulnerabilities in a weapon system and then have associated testing performed to thoroughly vet those problems in order to verify and characterize the vulnerabilities. A PM should be able to take CVA results and have confidence an exhaustive look at his/her program has been done. The PM can then take actions to mitigate the risks having a total cybersecurity picture. Another advantage of a proper CVA is documentation for future cybersecurity activities. Being able to know what has been examined and how the examination was performed should be valuable to future cybersecurity investigations, especially if new threats emerge. The knowledge of what has been evaluated in the past and what risk mitigation approaches were followed could help future cybersecurity personnel quickly focus on the emerging threat and determine if it will be a problem for the program.
4	I would like to have some continued visibility on how the DAU curriculum in training may be changing and if possible. "As opposed to a separate career field, maybe it's a, kind of think like...a dual major in where you could be a PM, but you can dual major in cyber. You could be a "loggie," and you can dual major in cyber. There's that level two, and level three, could be three and a half day classes or something that would be mixed like multiple functional, so it's not all PMs in the room, but so that everybody is going through a set curriculum as opposed to having five minutes of that slide being up on the board for level two PM and that's all we have." It looked like we were going to have a [cybersecurity] career field, but they are now integrating into the other career fields. For example, "being a logistics person with cybersecurity credentials specifically for logistics would be very valuable." Perhaps even a DAU training certificate for all career fields that shows you have some training/knowledge and add to one's other qualifications. New courses such as ISA 220 (RMF) and also working a software assurance course and many new workshops (promote a lot of questions and thinking)

Item	Concern
	to help fill these needs. The course in general are more policy oriented, but looking for something more in-depth with a problem-solving focus.
5	It has been very interesting listening to the people's perspectives. We operate in "cylinders of excellence" and sometimes you lose perspective on how different communities view this particular problem set.
6	Even though I am relatively new to cyber, I have my roots in the laboratory and admire the work of the technical testers/red teams that try to provide good feedback to the acquisition community.
7	I don't know where to go with this thing because it needs to be kept at a PIT system level, even though it has advantages to bring to the people at the higher levels who need to understand it too. Many great ideas and points brought up. When you get these ideas to a working stage there needs to be some studies to help determine what works and what doesn't work for the population you are servicing (data center vs. PIT, etc.). Metrics for learning are there, but they are tough because of the long connection between learning and production.
8	Keeping in mind this is not new, just that we need to do a better job of doing it. Need to understand the data owners, who the accrediting authorities are, defining the user population, with levels of concerns in order to design the security architectures accordingly. Also, teaching people that there are more then on pathways to accrediting a system. Some lose sight or are not aware at all. Treat cybersecurity like all the other "ilites" as it is prevalent through all of the specialties and should be treated very similar. I appreciate the opportunity to come and speak my mind and curious to see what comes out of this.
9	The longer RMA continues to evolve DIO and SEA they are currently so young that their requirements aren't consistent, but I appreciate everybody's point of perspective.
10	DAU has a big advantage as you reach more of the group and you can shift the water a lot more usefully that we can DoD-wide, where we are limited to our own competencies. "I think that cyber definitely is one of those ones that needs to be kind of like a working group, sort of lower-level kind of thing. If you just try to get it where you are teaching RMF or going through the 1,000 different check points you're just going to lose people." It's the kind of slide that everybody's eyes glaze over. It's kind of one of those you kind of have to work through, so going through a working group kind of thing or some sort of modified class schedule that would be where I think it needs to go." "Because the more people we can get DoD-wide about it like this vs. 'Oh, it's just a checklist I get and I'm done,' or 'cyber is just some fancy name for IA, it's all the same,' the better off we'll all be in the long run." Now I don't know a better to show them than bringing them all through it.
11	DAU is looking to put more exercises into the existing RMF courses. "The RMF thing is just a procedure, a high-level procedure. How you do it makes all the difference in the World." It's like encryption: It looks beautiful up on the shelf, but once you implement it, it can really be bad." Trying to get down to the working group, trying to get some hands-on, in RMF, so they can tell us why and make some sense to this and how are you going to contract that…." Need to be able to wrap their head around it and debate it logically. In the AFIT course on Avionics Vulnerabilities all feedback shows that the scenario run in the afternoon is very valuable. Most feedback shows the hands on portion is most useful. "As an alternative, a class that has well designed exercises and

Item	Concern
	one thing this has opened to me is having it include embedded systems, as well as enterprise level systems from a cyber thing and to make sure the exercises encompass both of those areas." Some work is currently being done in Engineering 301 where we do an exercise that is more CPI oriented and trusted system networks, but that is a crown jewel kind of analysis. From those exercises, we've found that many have trouble just identifying CPI. It's not a simple thing. It's not easy to look at a control and know what it is. It takes some effort. I like training engineers, but I would like to see a career field in this area as when you go higher than level 2 you are going to have to start specializing in embedded systems, or in aspects of test, or maybe even intrusion detection systems (IDS) or firewalls. "You could possible organize like hackers. Hackers don't know everything. They have specialists for certain functions."
12	"One of the madras we have at DAU is critical thinking and I think, what I'm hearing from each of you guys is critical thinking in cybersecurity is an absolute must, and that's why we have got to look a little bit different the way we [build] classes sometimes and this is leading to that. From my perspective this one-day workshop, as we've said this is an experiment. We had no idea, nothing has been done like this before that I'm aware of and had no idea on how it would come about. It has exceeded my expectations. I have picked up some really good nuggets of information and I do believe that we are going to take some of this back to the classroom. We are going to take this across our team, so I really want to thank you." "This is a tremendous group and I am very appreciative of you being here." "Tomorrow we are going to sit down and evaluate what we are going to do with this information. If we just cover the issues that have been brought up, I think we have a whole lot of information to look at and it's going to have an impact on us and the things that we are doing in the future."
13	"As an observer of this process...I think what you've created here, and I would urge you to take this back, is a great exercise particularly for Level 3 professionals certainly your Level 2, Level 3 professionals that this is the kind of adult education stuff that is really high impact on these sort of populations that takes very experienced people brings their experience into the classroom, has them participate in the learning, and has them leave not being told what to think, but in critical thinking terms being given a 'how to think' about a situation. So, I think what you've created is a very important learning exercise to take back to your different venues. Going to look different in different places, but in what we do in our center this is kind of high-impact stuff for particularly senior people that really makes a difference in organizations." Thank you for your time today. "It not only helped us tease out the things of what needs to be addressed in terms of gaps as we are looking through what kind of cybersecurity issues are throughout the acquisition cycle, but I hope it helped you also to be able to interact with other career fields and backgrounds and be able to network and those types of things that get things done."

Appendix G: **DAU Secure System Design Course Experiment Data Sheet**

Please fill out the following participant background information in order to help in data capture for follow-on analysis:

Name: ___________________________________

Email: ___________________________________

Phone: ___________________________________

Occupation(s) (e.g. Engineer, Program Manager, etc.):

____

Previous Occupational Experience (e.g. System Design, Operational Test and Evaluation, etc.):

____

____

____

____

____

____

____

____

____

____

Previous DAU Course Experience:

____

____

____

____

____

____

____

____

____

____

Previous Cybersecurity Training/Education/Certifications Outside of DAU (e.g. CISSP, etc.):

Previous Cybersecurity Experience:

1. In your experience, what are some of the most pertinent cybersecurity issues currently in the acquisition cycle?

2. In your experience, what key gaps have you observed in DAU curriculum having to do with cybersecurity issues in acquisition?

Appendix H: **Pre-Proposed Questions to Drive Discussion**

Questions to Ask at Each Milestone

1. What cybersecurity functionalities are actually needed?

2. What is your role/responsibility in this area?

3. Who are the people that should also be engaged?

4. Where is it important to use cybersecurity experts?

5. What are the interdependencies? How could a compromise in system “x” affect “y”?

6. How does this affect RFP/SOW/Contract wording?

Learning Needs / Key Technical Sub-System Cybersecurity Questions

7. What are the requirements for sub-system documentation and what are open source research techniques?

8. How do I identify the cybersecurity relevant support, training, lab and maintainability factors required for functionality?

9. How do I identify the cybersecurity relevant ports, protocols, messaging, power, space, cooling, etc. delineated for functionality?

10. How to recognize the key RMF controls germane to different platforms and applications (CAA – Cyber Applicability Assessment)?

Vulnerability Analysis

11. How do I identify of sub-system mission criticalities and vulnerabilities?

12. What are the equities of Anti-tamper and cybersecurity?

13. How to identify the critical elements in SW and HW that would allow access and changing of the code or HW integrity, or execution of unauthorized code?

14. How to rapidly rank cybersecurity access and vulnerabilities?

Solutions Analysis

15. How to identify limitations, unintended consequences (Pharmaceutical Effects) and tradeoffs of proposed cybersecurity mitigations?

16. How to identify information that highlights vulnerabilities for cybersecurity mitigations?

17. How to evaluate unintended and malicious data input for probability and impact?

18. How to identify equities and out of band verification?

19. How to identify hidden or unintended (or unused) functionality (MacGyver Effect)? How to minimize SW functionality?

Cybersecurity Test

20. What are the security requirements of cybersecurity tools?
21. How to evaluate unintended and malicious data input for probability and impact?

22. What are the qualifications of a cybersecurity test team?

23. What are the criteria and capabilities for lab, SIL, range, JIOR, or NCR for division of cyber test events?

24. How do I integrate and support Cybersecurity, Anti-tamper, Supply chain and SwA testing across different organizations and schedules?

25. What are the security concerns and classification of test data, tools, techniques, etc.?

26. How do I evaluate cybersecurity DT results and recommend mitigations, follow-on test and shape Red Team OT test scope?

27. How do I evaluate Adversary intent, capability and threat credibility? How to identify the appropriate level of Adversary capability and Red Team ROE?

28. How do I evaluate cyber-attack mission impact in terms of critical mission functions / objectives?

29. What are the test methods and implications for Cybersecurity Survivability Attributes?

Appendix I: **DAU Course Experiment Participant References**

1. DoDI 5000.02, "Operation of the Defense Acquisition System" Enclosure 14, p. 170,
    a. Especially p. 179, Item #7 "Program Manager and Component Actions to implement Cybersecurity and Related Program Security Across the Material Lifecycle." http://www.dtic.mil/whs/directives/corres/pdf/500002_dodi_2015.pdf
2. "The DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle." Version, 1.0, September 2015. https://acc.dau.mil/CommunityBrowser.aspx?id=721696
    a. Pre-Milestone A - Prior to MDD – (p. 24-30)
    b. Milestone A – (p.31-33)
    c. Milestone B – (p.34-37)
    d. Milestone C – (p.38-41)
    e. Review all annexes
3. DoDI 8500.01, "Cybersecurity," March 2014. http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
4. "The Cybersecurity & Acquisition Lifecycle Integration Tool (CALIT)," Version 2.02 (Overall Reference). https://acc.dau.mil/CommunityBrowser.aspx?id=740975
    a. Pre-Milestone A - Prior to MDD – Slides 1-6
    b. Milestone A – Slides 7-9
    c. Milestone B – Slides 10, 11, 12
    d. Milestone C – Slides 13, 14, 15, 16, 17
5. Defense Science Board 2013 - http://www.dtic.mil/docs/citations/ADA569975
6. Implementation for Cyberspace Survivability **(will send via AMRDEC SAFE)**
7. Avionics Cyber Vulnerability Assessment and Mitigation Manual **(will send via AMRDEC SAFE)**
8. Avionics Cyber Hardening And Resiliency Manual **(will send via AMRDEC SAFE)**
9. Unified Facilities Criteria (UFC) 04-010-06 **(will send via AMRDEC SAFE)**
10. Report of the Defense Science Board Task Force on Cyber Supply Chain, February 2017 https://www.erai.com/CustomUploads/ca/wp/DSB-CyberSupplyChainReport-Final.pdf
11. Cybersecurity T&E: https://acc.dau.mil/CommunityBrowser.aspx?id=738843&lang=en-US
12. DoD Cybersecurity T&E Guidebook, 1 Jul 15, https://acc.dau.mil/CommunityBrowser.aspx?id=738843&lang=en-US

Appendix J: Parking Lot Issues

As part function as facilitator of the event and discussions, CSIAC established a “Parking Lot” for topics that came up in the course of discussion that were currently beyond the focus of the current event, but may provide merit later. They are documented for possible future reference.

Parking Lot:

- Attestation

- OMS openness and versatility vs. increased susceptibility and vulnerabilities

- How will the process be implemented as requirements are pushed to the left. Probably start out as a less related checklist. Balance between agility and stability.