



# SYSTEM SECURITY ENGINEERING (SSE) CHALLENGES IN THE CYBER SPECTRUM



Rodney Visser  
DAU South Cyber Guy  
[rodney.visser@dau.mil](mailto:rodney.visser@dau.mil)  
256.922.8709

[www.DAU.mil](http://www.DAU.mil)

# Overview

- **Cyber Security Landscape**
  - 2 Opposing Forces
- **Why we need change?**
  - DOT&E Annual Reports
- **What we need to change:**
  - Regulation
  - Contract Language
  - Implementation
- **Plan to effect change!**
- **How DAU and our partners “Full Duplex” Cybersecurity Support can help!**



# Cyber Security Posture



VS

**ORACLE®**



# DOT&E FY 2014 Annual Report

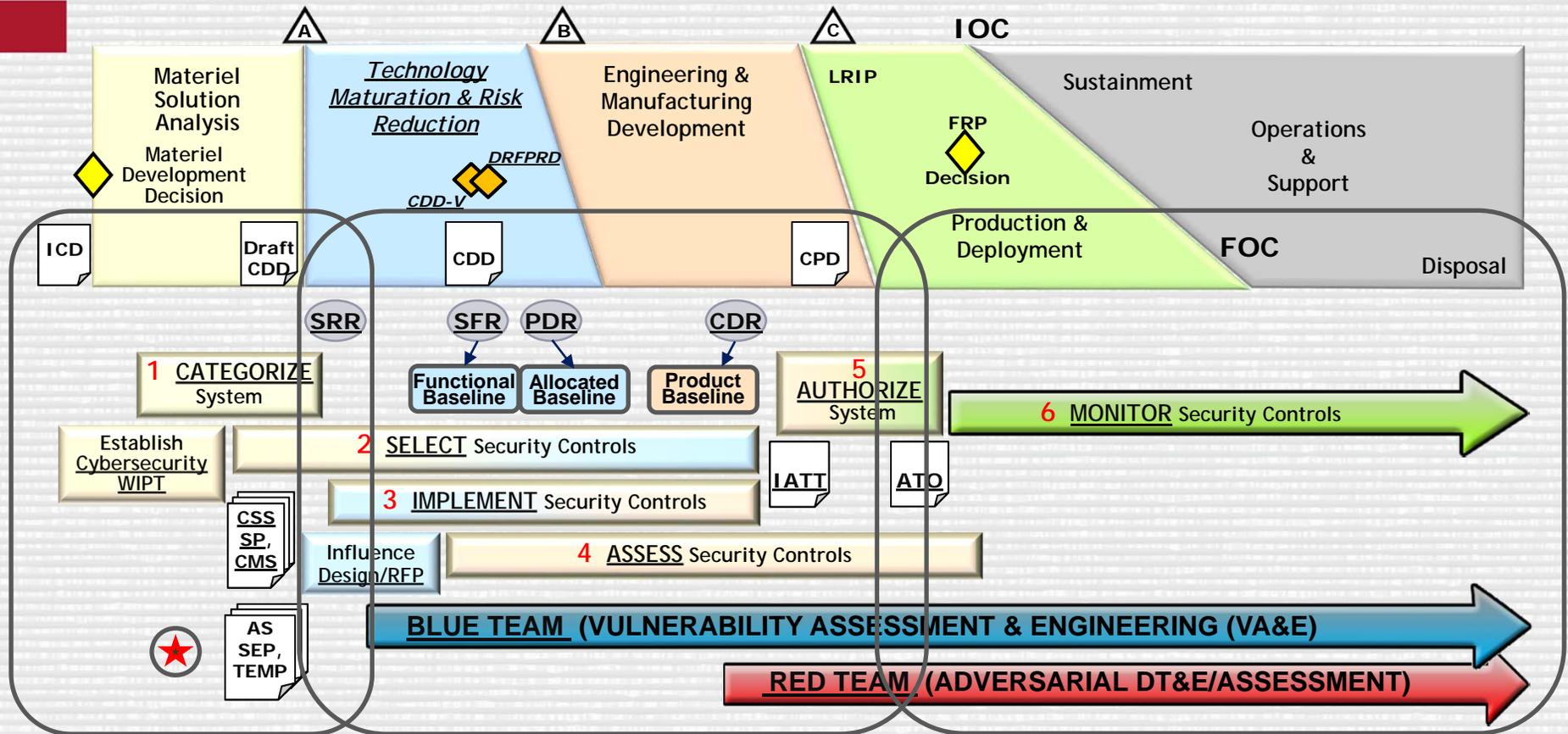
- “Cyber adversaries have become **as serious a threat** to U.S. military forces as the air, land, sea and undersea threats represented in operational testing for decades”
- “Program managers worked to resolve vulnerabilities found from cybersecurity testing in prior years, **but FY-14 testing revealed new vulnerabilities.**“
- “Cyber Opposition Forces (OPFOR) portraying adversaries with beginner or intermediate cyber capabilities were able to demonstrate that **many DOD missions are currently at risk from cyber adversaries**”
- “Demand has begun to **exceed the capacity of existing personnel** able to portray cyber threats.”

**Offensive cyber capabilities are evolving rapidly**

Source: DOT&E FY 2014 Annual Report  
(January 2015)



# Cybersecurity/RMF Integration across the Acquisition Lifecycle



We need to change the regulations that govern security requirements.

We need to update the contract language to combat common threats.

We need to do a better job implementing security controls throughout the life cycle.



# Integrating Cybersecurity into our Acquisition Programs

- **How effective has DoD been to date on integrating Cybersecurity into our acquisition programs?**
  - DoD consistently “bolts on” Cybersecurity later in the design process at great cost while achieving marginal results (FY2014 DOT&E Report)
  - Without a new/different approach we can expect similar or worse results
- **Could ensuring Cybersecurity is part of the design process improve results?**
  - Leaders and Team members (Gov’t & Industry) must make this a priority
- **Some keys to success:**
  - Treat Cybersecurity as a true design consideration – “Design for Cybersecurity”
    - This is already done for supportability/sustainability, why not for Cybersecurity?
  - Get leadership on board early – Cybersecurity impacts overall program risk!
  - Get the entire team on board – Cybersecurity is a “team sport”
  - Ensure your Industry Partner(s) have a solid track record on Cybersecurity
    - Use Cybersecurity in the Source Selection process (Past Performance, etc) to help to differentiate among the offerors
  - Develop and incorporate Cybersecurity related contract language to get better results





U.S. AIR FORCE

# Acquisition Cyber Resiliency Campaign Plan



SMC



AFLCMC



NWC



AFRL

LOA 1: Mission Thread Analysis	LOA 2: Integrate into SE Process	LOA 3: Cyber Workforce Development	LOA 4: Enhance Adaptability	LOA 5: Develop Common Security Environment	LOA 6: Assess and Fix Legacy Systems	LOA 7: Intelligence for Cyber Security
End-to-end operational process supporting a mission	Incorporates systems security engineering into all phases of the acquisition life cycle	A cyber-savvy workforce capable of integrating cyber security measures into all phases of the acquisition process	Vigorously enhances the adaptability of our weapon systems to rapidly respond to threats	Facilitates the integration of cyber security measures into all phases of the acquisition process	Prioritizes legacy systems to fix existing and future cyber vulnerabilities	Strengthen acquisition cyber security through improved intelligence collection, analysis, and application

## Mission Assurance End State

Resilient Systems

Common Processes

Educated Workforce

High Confidence Missions



## Draft *National Initiative for Cybersecurity Education (NICE) KSAs* from National Cybersecurity Workforce Framework

Item ID	KSA	Statement	Competency
22	KSA	* Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
108	KSA	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management
1157	KSA	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	Legal, Government, and Jurisprudence
1158	KSA	* Knowledge of cybersecurity principles.	Information Systems/Network Security
1159	KSA	* Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment

Initial <u>Cyber Basics</u>	After Cyber Basics <u>Cyber Policy &amp; Threats</u>	Post Classroom <u>Cyber Risk Management</u>
<ul style="list-style-type: none"> <li>• <b>Networking Concepts (KSA – Infrastructure Design) - 3 Hours Online</b></li> <li>• <b>Cybersecurity Principles (KSA – Info Systems/ Network Security) - 4 Hours Online</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Cyber Threat (KSA – Vulnerability Assessment) - 3 Hours Classroom</b></li> <li>• <b>Cyber Policy (KSA – Legal and Governance) - 3 Hours Classroom</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Cyber Risk Management (KSA – Risk Management use ISA 220) - 6 Hours Online</b></li> </ul>
<b>These Core NICE KSAs are For AWF Career Fields</b>		





# How DAU Can Help



# How DAU Can Help

- **DAU is a “full duplex” organization** – We listen to our customers to ensure we understand your challenges and to learn about how to better meet your needs – This is especially true when it concerns Cybersecurity.
- **Education**
  - Student Centered learning + skilled listening
  - Every customer engagement is an opportunity for DAU to learn
- **Collaboration** - We are members of our local community and pride ourselves in supporting you
- **Execution** – We do Mission Assistance! It one of our core competencies. We help our customers solve their acquisition challenges at the point of need
- **Expertise** – We are investing in our Cybersecurity expertise – Cybersecurity new hires



# Questions?

Rodney Visser  
DAU South Cyber Guy  
[rodney.visser@dau.mil](mailto:rodney.visser@dau.mil)  
256.922.8709

