THE UNIVERSITY OF MEMPHIS

Systems Testing Excellence Program

Cyber Security, Testing, and Universities

Systems Testing Excellence Program (STEP)

By
Dr. Robin Poston, Associate Director of STEP
2nd Cyber Security Workshop Program
February 2015

Step.Memphis.edu

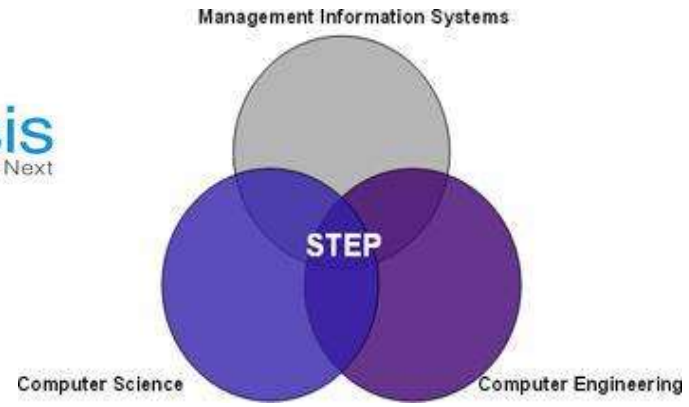
A Partnership for Advancing the Science of Testing

System Testing Excellence Program

FedEx

Mphasis
Unleash the Next

SYNTEL
Consider IT Done



DISA
A Combat Support Agency

ELSEVIER

APPLAUSE
WINNING APPS GET IT

LOCKHEED MARTIN

NRI 未来創発
Dream up the future.

COOK SYSTEMS INTERNATIONAL INCORPORATED

CISCO

AutoZone

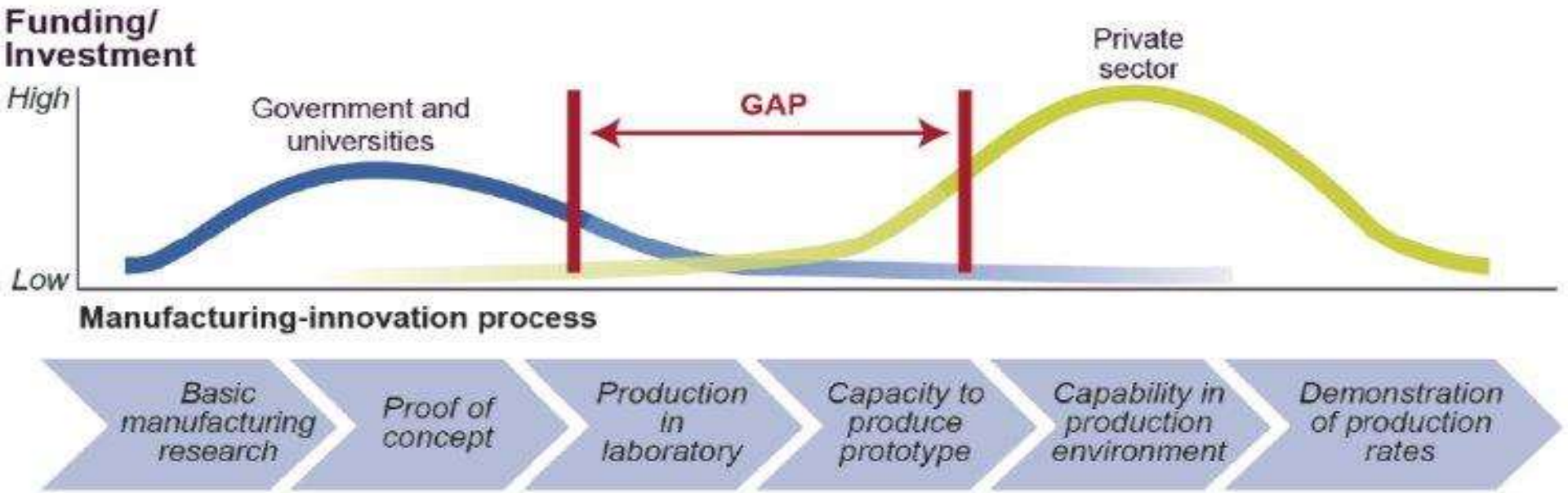
Thomas&Betts

Types of Cyber Security Testing

- Functional Testing
- Regression Testing
- White/Black/Grey Testing
- Decision table Testing
- Path Testing
- Infrastructure Testing
- Data flow Testing
- Requirements Testing
- Control flow Testing
- End-to-end Testing
- Configuration Testing
- Load Testing
- Iterative/Incremental Testing
- Unit Testing
- Application Security Testing
- Fuzz Testing
- Component testing
- Production system testing
- Source code testing
- Penetration testing

Academic Research Study Efforts

Reference	Cyber Security Research Topics	Impact On Software Development, Engineering, and Testing
Ashford, Warwick, 2013	Third party monitoring	MS tool to help disruptive assaults on its products
Jackman, Stephen, 2010	Issues on information security	Considering security within software development is being implemented
Dunkel, Dan, 2009	Silo thinking	Correlation of silo thinking and cybercrime
Ashford, Warwick, 2010	Password system named Gaia	How Gaia system able to gain access to Google
Greenberg, Andy, 2011	Investigation tool	Alpha version of a system that would allow placing of bets on questions in information security
Zolfagharifard, Ellie,2014	Vulnerability issues	Vulnerability of the Internet of Things to attack and hackers' ability to control an internet-enabled device
Maughan, Douglas, 2010	Importance of the U.S. R&D	Security of the nation's digital and information infrastructure
Ritchey, Diane, 2014	Cyber security breaches	Discusses about tools used in mitigating data threats and cyber crime
Rice, Jim, 2014	Need of ongoing monitoring system	Importance of supply chain innovation in response to threats of cyber security
Chabinsky, Steven, 2014	Benefits of cloud-based security	Security in cloud computing technology



Research model:	**NSF/NIH/other Grants** focused on specific industry – wide challenges (non-commercializable)	**Cyber Security Contract Research & Training** using science to examine specific challenges *	**R&D** focused on business sustainability and return on investment (commercializable)

* STEP addresses the GAP in systems testing as academics work with government agencies and private companies to develop new ideas about the specific challenges. Our research provides input for our training programs, back to the organizations for process innovation, and published papers to generate more knowledge.

Cyber Security T&E Research and Training

- Why is this important?
  - Existing processes have been ineffective
  - Cybersecurity T&E, Systems Security Engineering (SSE), and Risk Mgmt Framework (RMF) processes must be aligned and mutually supportive
  - DT&E should provide feedback as early as possible
  - OT&E outcomes will be better
- Work in progress?
  - Overview DOD Cybersecurity T&E Phases
  - Discuss Cyber Evaluation Framework
  - Overview National Cyber Range
  - Walk through a simple example and have fun!

STEP Research-Based Certifications and Workshops with Cyber Security T&E

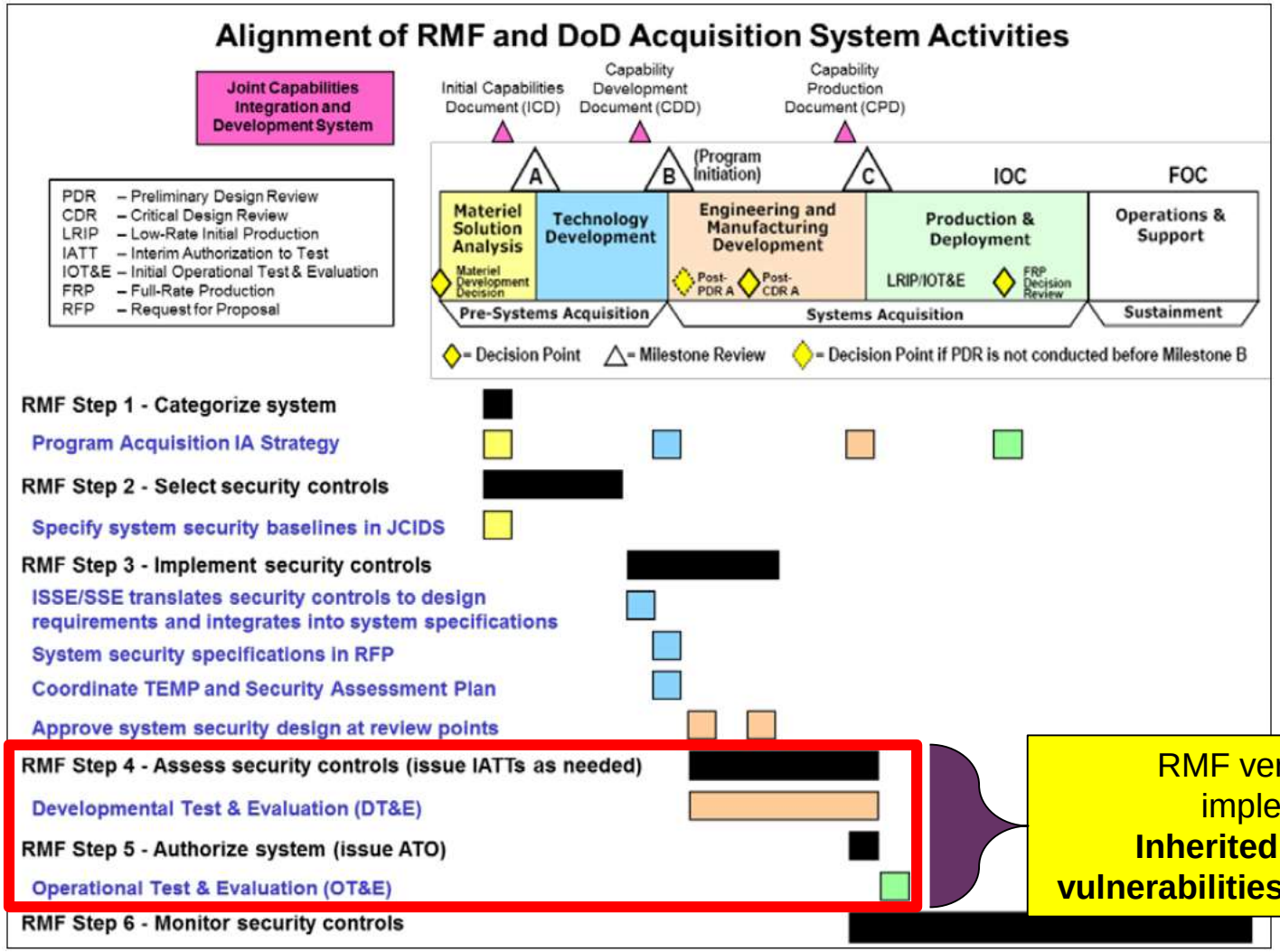
- Foundational Certification in Systems Testing
  - —Five Days (10 half-day modules and exam)
- Advanced Certification in Systems Testing
  - —Ten Days (20 half-day modules and group project)

- Will host 9th International Research Workshop on Advances and Innovations in software testing, and Annual ITEA Technology Workshop

Cyber Security Problems

- System vulnerability (Ellie, 2014)
- Security analysts and testers lacks enough skills (Warwick, 2010)
- Dearth of security testing workforce (Libick et al., 2014)
- Education/training is lacking (Maxson, 2013)

DOD RMF Necessary But Not Sufficient To Understand Systems Cybersecurity Posture!



RMF verifies controls implementation **Inherited and Residual vulnerabilities often overlooked!**

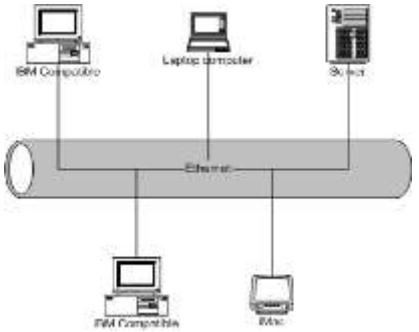
Graphics Source: DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT: Issued 14 Mar 2014

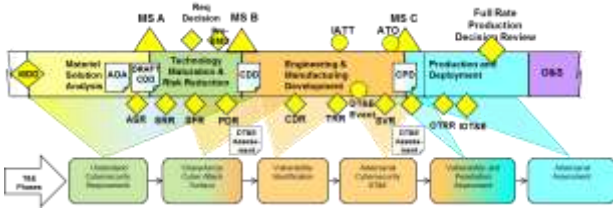
Cyber Security Challenges

- Criminals/hackers are winning (Diane, 2014)
- Security departments are behind (http://www.brookings.edu; http://rt.com/usa/)
- New technology introduces new challenges
  - Cloud computing (Sen, 2013)
  - Big Data (Cloud security alliance, 2012)
- Security testing tools exist, but are they efficient and effective**?**

Improving Cyber Security T&E

- Cybersecurity T&E must be mutually supportive of Systems Security Engineering
  - Involves all “responsible” stakeholders
  - Started as early as possible in Acquisition
  - Provides early feedback to “responsible” stakeholders
  - Evaluates Security Architecture and exposed “Attack Surface”
  - Confirms baseline requirements and verifies controls
  - Goes beyond verification to identify exposed vulnerabilities
  - Adversarial assessments evaluate system resilience in operational context
  - Ultimately reduces cost, improves schedule and performance





University Can Help

- Offer education/training based on forward thinking ideas for security analysts and testers (Locasto et al., 2011)
- Perform research on improving security tools, software, and processes (http://www.sei.cmu.edu; http://www.dhs.gov; http://info.law.indiana.edu)
- Host think-tank consortia of the leading thought-leaders to explore best practices and share their expertise on cyber security testing (McGettrick, 2013)

References

1. Zolfagharifard, Ellie, 2014, "Beating the bugs", Engineer (Online Edition). 10/17/2014, p1-1. 1p.
2. Ashford, Warwick, 2010, "Untitled", Computer Weekly, p11-11. 1p.
3. MARTIN C. LIBICK et al 2014, "H4CKER5 WANTED".
4. Margaret "Peggy" Maxson, 2013, "How to use the National Cybersecurity Workforce Framework"
5. Ritchey, Diane, 2014, "Cyber Risk and Special Security Report", Security: Solutions for Enterprise Security Leaders, Vol. 51 Issue 2, p40-46. 5p.
6. http://www.brookings.edu/blogs/techtank/posts/2015/02/3-cybersecurity-federal-it-plans
7. http://rt.com/usa/state-department-no-cyber-security-823/
8. Jaydip Sen, 2013, "Security and Security and Security and Privacy Issues in Cloud Computing".
9. Cloud security alliance, 2012, "Top ten big data security and privacy challenges".
10. Michael E. Locasto et al 2011, "Producing an Expert Cyber-Security Work Force from Thin Air", vol.54:no.1.
11. http://www.sei.cmu.edu/security/
12. http://www.dhs.gov/st-snapshot-swamp-key-resource-improving-software-assurance-activities
13. http://info.law.indiana.edu/releases/iu/2014/02/swamp-cybersecurity-resource.shtml