

# Difficulties In Evolving the Cybersecurity Workforce: As Clear As A.I.R (Archaic Ineffective Requirements)

Corey T. Jackson, MBA, CISSP, CSSLP, NET+  
Senior Enterprise Knowledge Architect  
US Department of Justice- Federal Bureau of Investigation

# 2010 FISSEA Conference

- Our Path
- Our Destination
- Cybersecurity Personnel Requirements
- Case Studies/Frameworks/Matrices/Models
- What Now
- What Next
- Questions

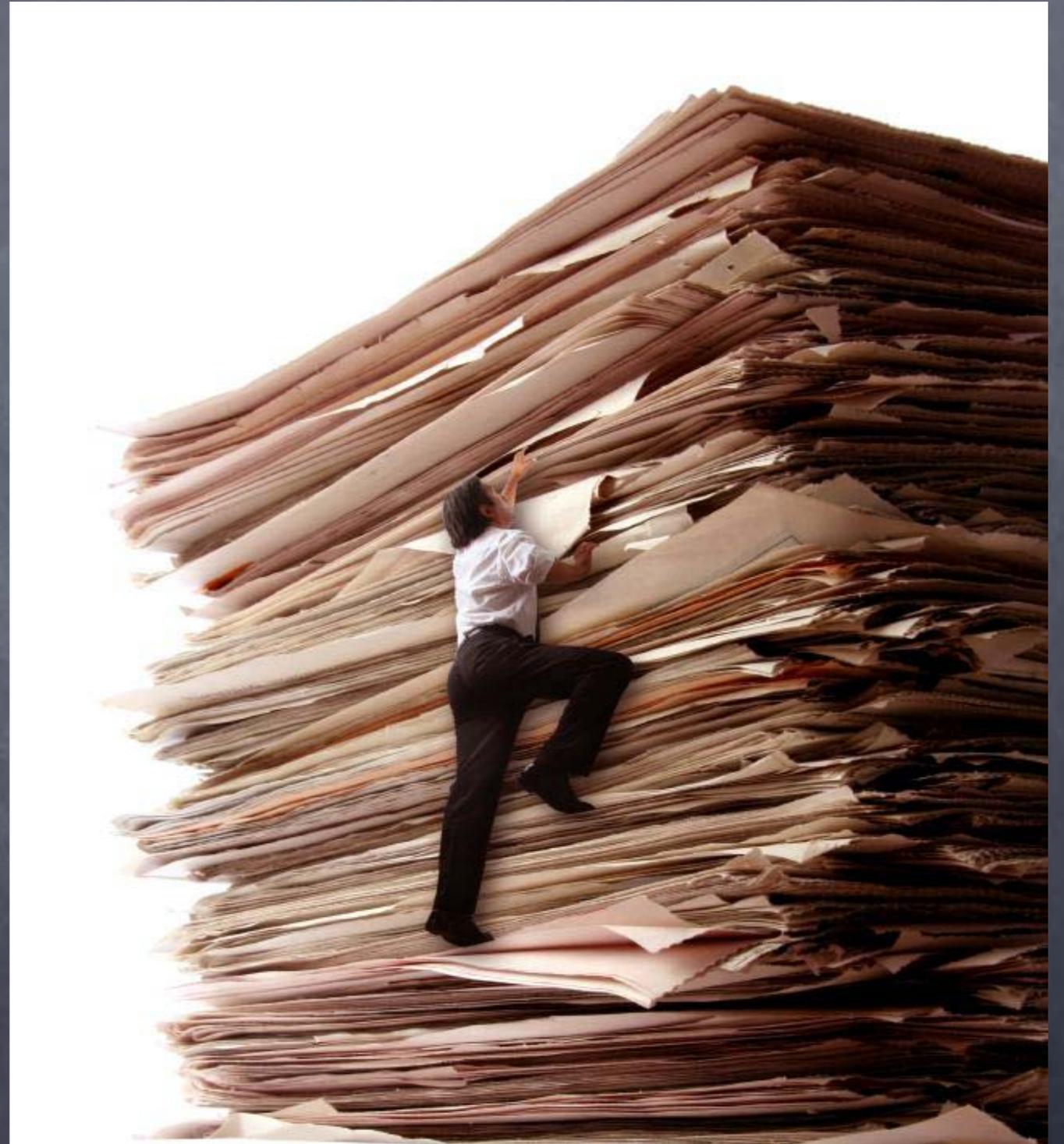
*“It is pardonable to be defeated, but never to be surprised.”*

*Frederick the Great King of Prussia (1712-1786)*

# Our Path

## What Governs Our Requirements

- ✓ US Office of Personnel Management (OPM)
- ✓ Office of Management and Budget (OMB)
- ✓ Federal Information Security Management Act of 2002 (FISMA)
- ✓ National Institute of Standards and Technology (NIST)
- ✓ The Committee on National Security Systems (CNSS)
- ✓ Industry (ISC<sup>2</sup>, CompTia, GIAC, etc)
- ✓ Individual organization/agency standards



# Our Destination

Governance  
OMB/FISMA/CNSS  
DIACAP

Authority  
OPM/NIST/NSA  
DHS/GSA

Human Capital  
Collaboration/Processes  
Education/Training

**“CYBERSECURITY  
ECOSYSTEM”**

Certifications  
ISC<sup>2</sup>/GIAC/CompTia  
ISACA/SCP

Degree  
IA/CompSci/Comp Eng  
InfoSys/MIS

# *Cybersecurity Personnel Requirements*

- Academia
- Human Capital
- IT Security Manager
- IT Security Professional
- DoD/Federal Civilian/Intelligence  
Community/Corporate

# Case Studies/Frameworks/ Matrices/Models

- NIST SP 800-16
- DHS EBK
- DoD 8500
- Federal CIO Council
- Dissertation



**IT Security EBK:  
A Competency and Functional Framework**

Functional Perspectives  
M - Manage  
D - Design  
I - Implement  
E - Evaluate

	IT Security Roles												
	Executive			Functional					Corollary				
	Chief Information Officer	Information Security Officer	IT Security Compliance Officer	Digital Forensic Professional	IT Systems Operations and Maintenance Professional	IT Security Professional	IT Security Engineer	Physical Security Professional	Privacy Professional	Procurement Professional			
1 Data Security	M	M	D			I	E	M	D				
2 Digital Forensics				M	D								
3 Enterprise Continuity	M	M											
4 Incident Management	M	M	D			I	E					M	D
5 IT Security Training and Awareness	M	M	E										
6 IT Systems Operations and Maintenance					E	D	M	D					
7 Network and Telecommunications Security					E	I	E						
8 Personnel Security	M	M											D
9 Physical and Environmental Security	M	M										M	D
10 Procurement	M	D	M	D									M
11 Regulatory and Standards Compliance	M	M	D										E
12 Security Risk Management	M	E	M	D									M
IT Security Competency Areas													
IT Security Management	M	D	M	D									
Information Security	M	M	E										



# *What Now ?*

- Incentives
- Assessments (Amnesty)
- Preceptor Programs
- Contact Hours
- Certification vs. Licensure
  - Standards/Theory/Capability

# *What Next ?*

- What do we not know?
- How do we gauge competence?
- How do we collaborate?
- How do we migrate?
- Means to “regulate”
  - Cybersecurity Act of 2009

*Questions???*



*Contact info: [corey.jackson@ic.fbi.gov](mailto:corey.jackson@ic.fbi.gov) 301-429-3672*