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."

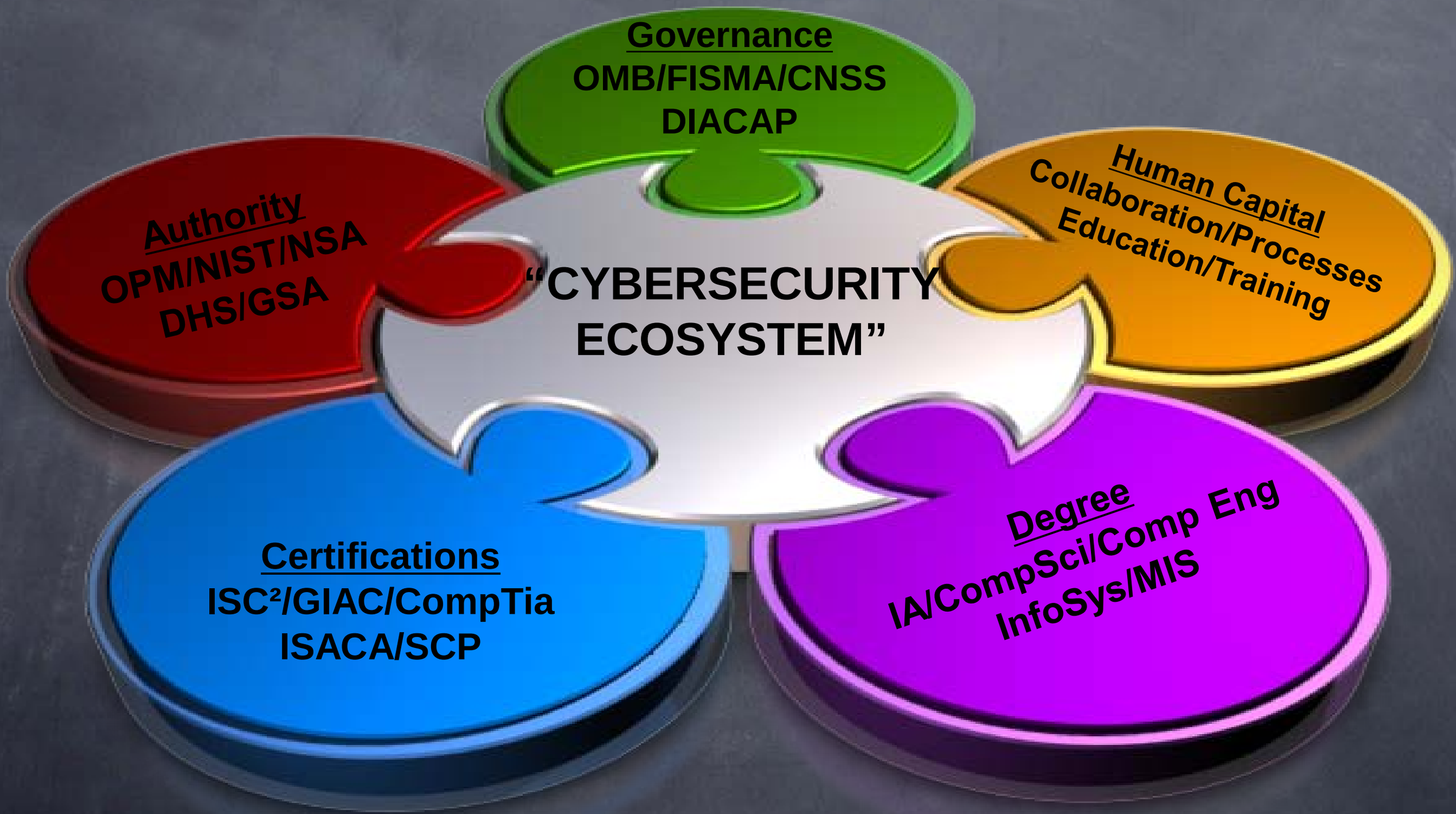
Frederick the Great King of Prussia (1712-1786)

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 (ISC², CompTia, GIAC, etc)
- ☑ Individual organization/agency standards

Our Destination

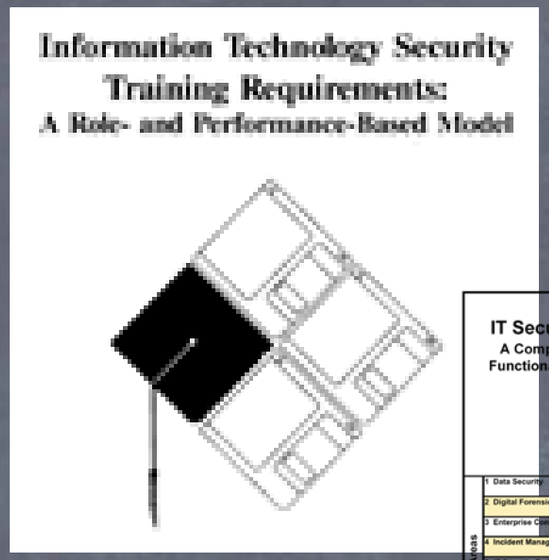


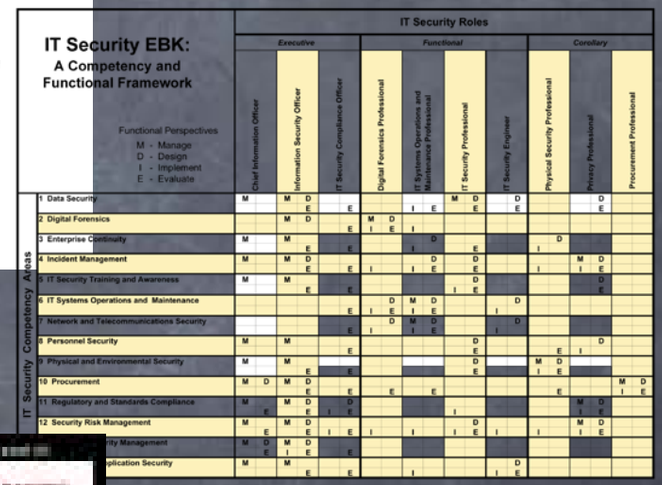
Cybersecurity Personnel Requirements

- 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





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 301-429-3672