



# A Systems Approach to Protecting the U.S. Air Traffic Control System Against Cyber-Terrorism

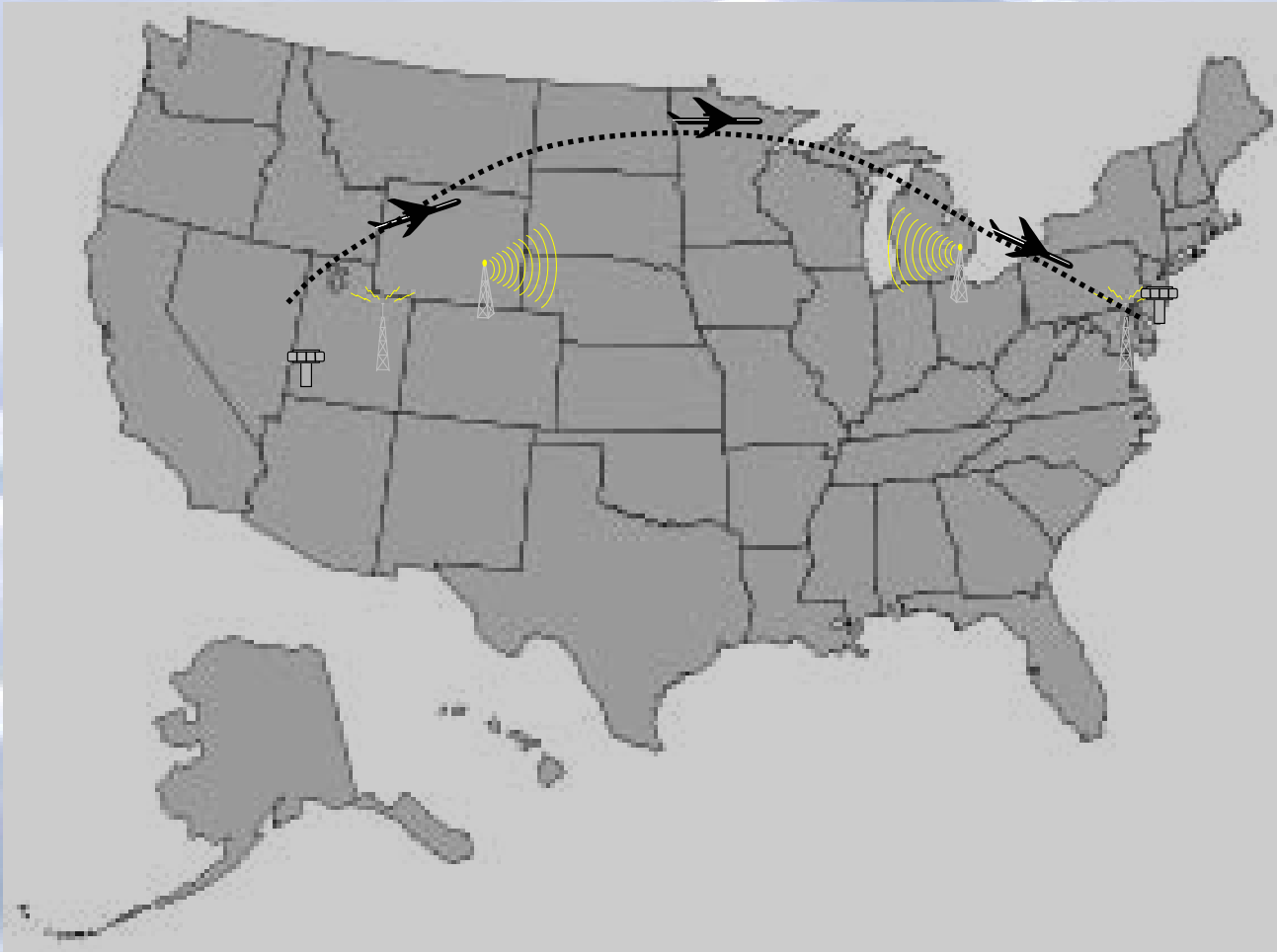
**Arthur Pyster**

*Deputy Assistant Administrator for  
Information Services and  
Deputy Chief Information Officer  
[arthur.pyster@faa.gov](mailto:arthur.pyster@faa.gov)*



# *The FAA's Job*

**Each day, manage 30,000 commercial flights to safely move 2,000,000 passengers and 60,000 tons of cargo**



- ~ 500 FAA Managed Air Traffic Control Towers
- ~ 180 Terminal Radar Control Centers (low altitude)
- 20 Enroute Centers (high altitude)
- ~ 60 Flight Service Stations (general aviation)
- ~ 40,000 Radars, Navigational Aids, Radios, ...



## *The Threat*

“It is important to concentrate on the destruction of the American economy...”

*Osama bin Laden*

“If there had been a cyber-attack at the same time [September 11] that prevented them [air traffic controllers] from doing that [bringing down the aircraft], the magnitude of the event could have been much greater.”

*Ron Ross, Director of the National  
Information Assurance Partnership*

“The event I fear most is a physical attack in conjunction with a successful cyber-attack on the responders’ 911 system or on the power grid.”

*Ron Dick, Director of FBI National  
Infrastructure Protection Center*



## *FAA's Systems Approach*

- Establish strategy, policy, and guidance
- Systematically and continually examine threats and vulnerabilities
- Create an information systems security architecture that responds to those threats and vulnerabilities
- Implement information systems and networks consistent with the architecture
- Establish, institutionalize, and continuously improve processes
- Deploy security measures incrementally
- Monitor compliance and measure progress
- Manage risks proactively at each major decision point

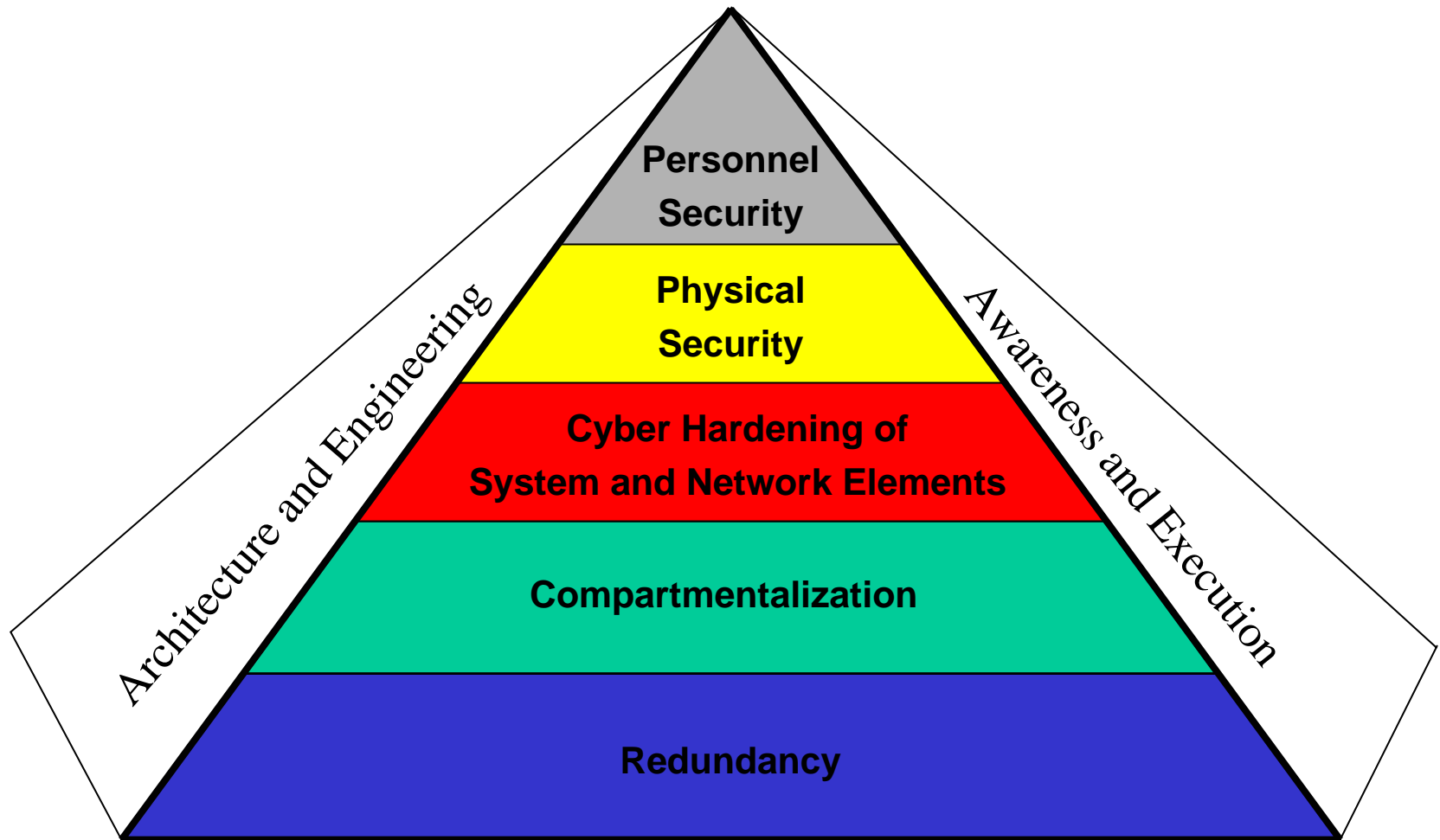


# *FAA's Cyber Defense Strategy*

- Harden individual system and network elements
  - Make it difficult to knock out individual elements, but recognize that successful attacks may occur
- Isolate elements to avoid “viral” spread
  - Build on the FAA infrastructure that is already designed to tolerate independent failure of system and network elements
  - Recognize that cyber attacks can be “viral” in nature, impacting a swath of elements
  - Create firebreaks within the network to minimize viral spread
  - Monitor networks to detect attacks and impose additional containment
- Back up key elements to avoid service disruption
  - Build on the fact that redundancy is already integral to achieving safety and performance with the FAA infrastructure
  - Develop recovery and restoration procedures that include cyber events

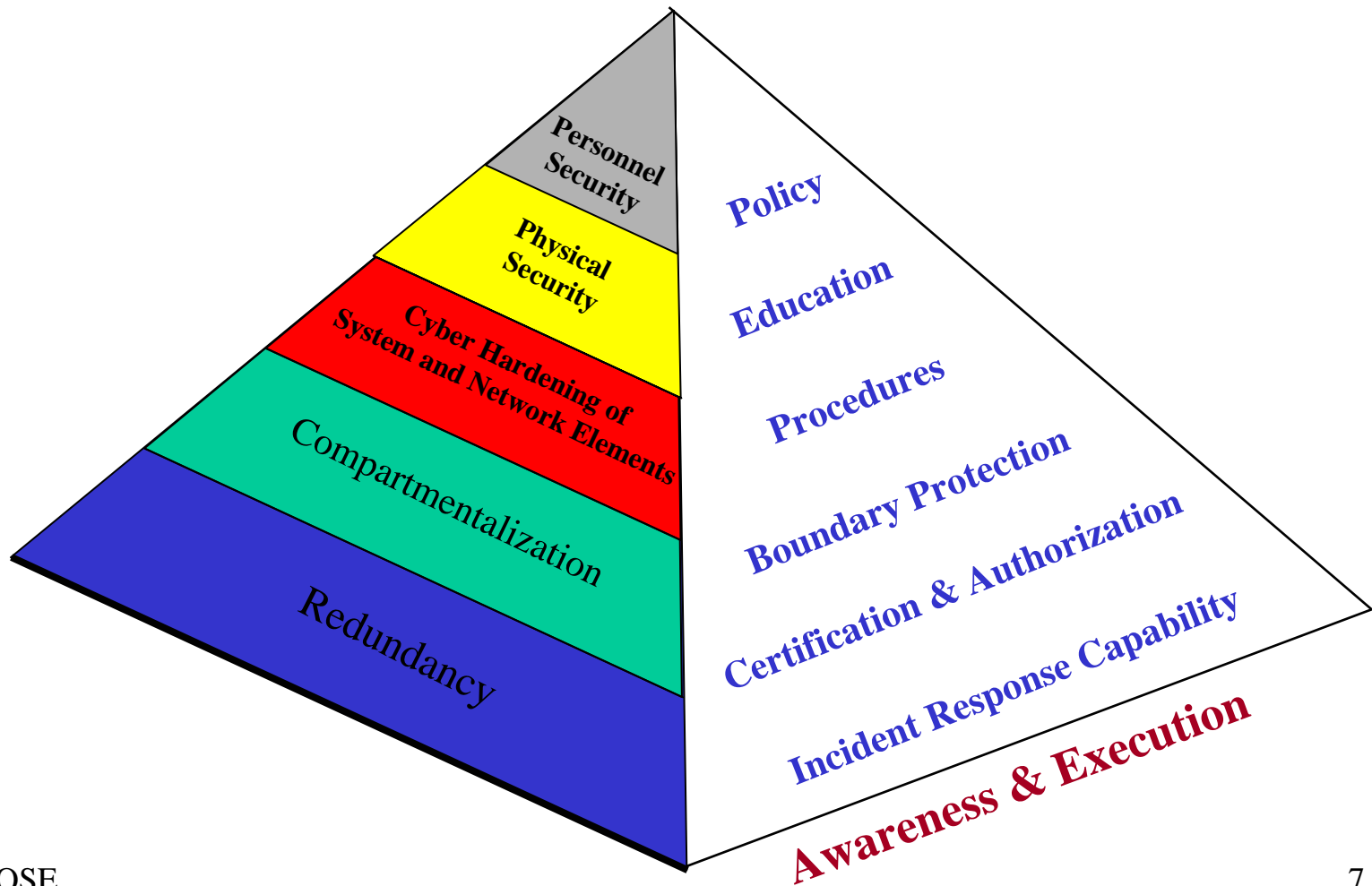


# *FAA's 5 Layer Enterprise Security Model*



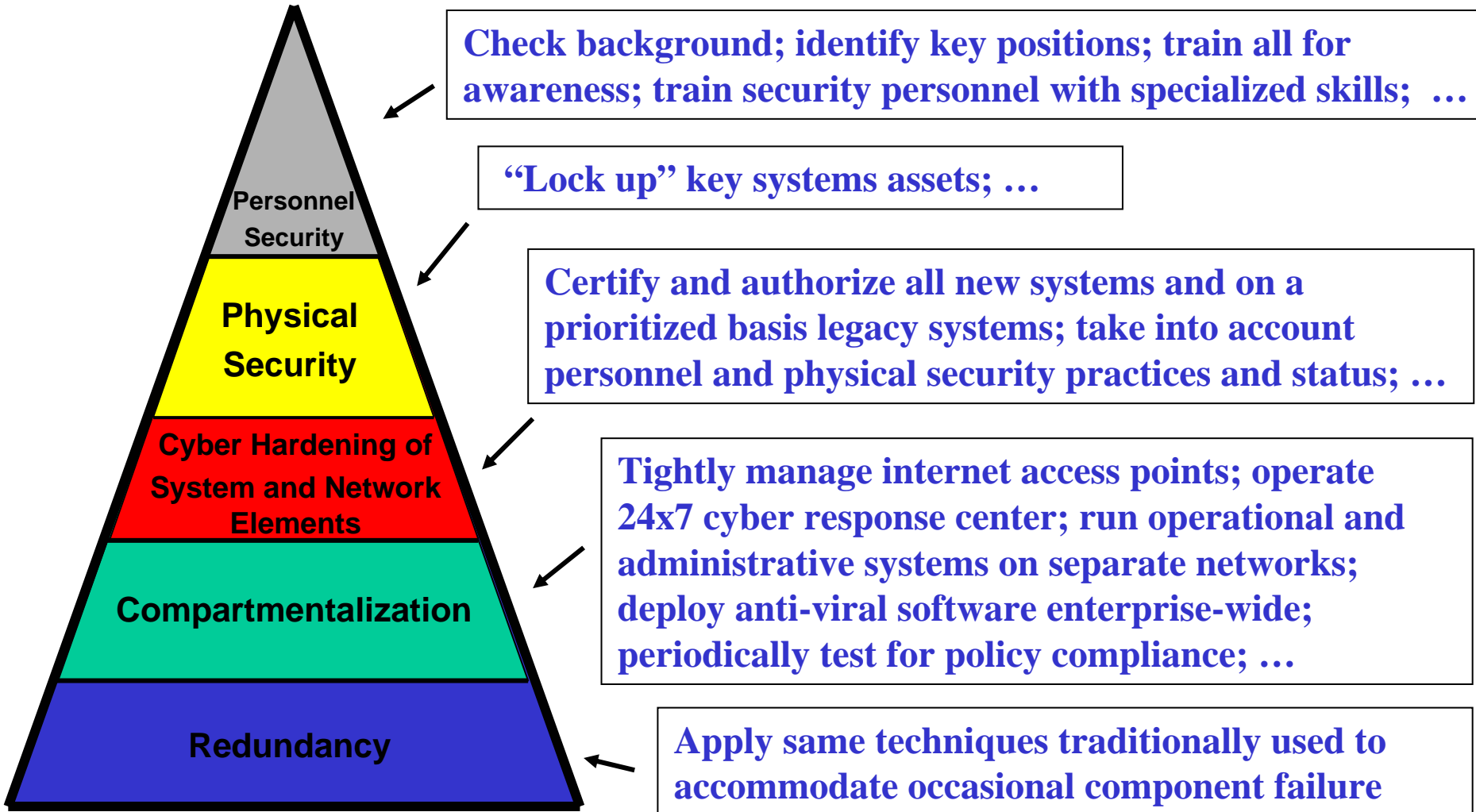


# *Awareness and Execution Perspective*



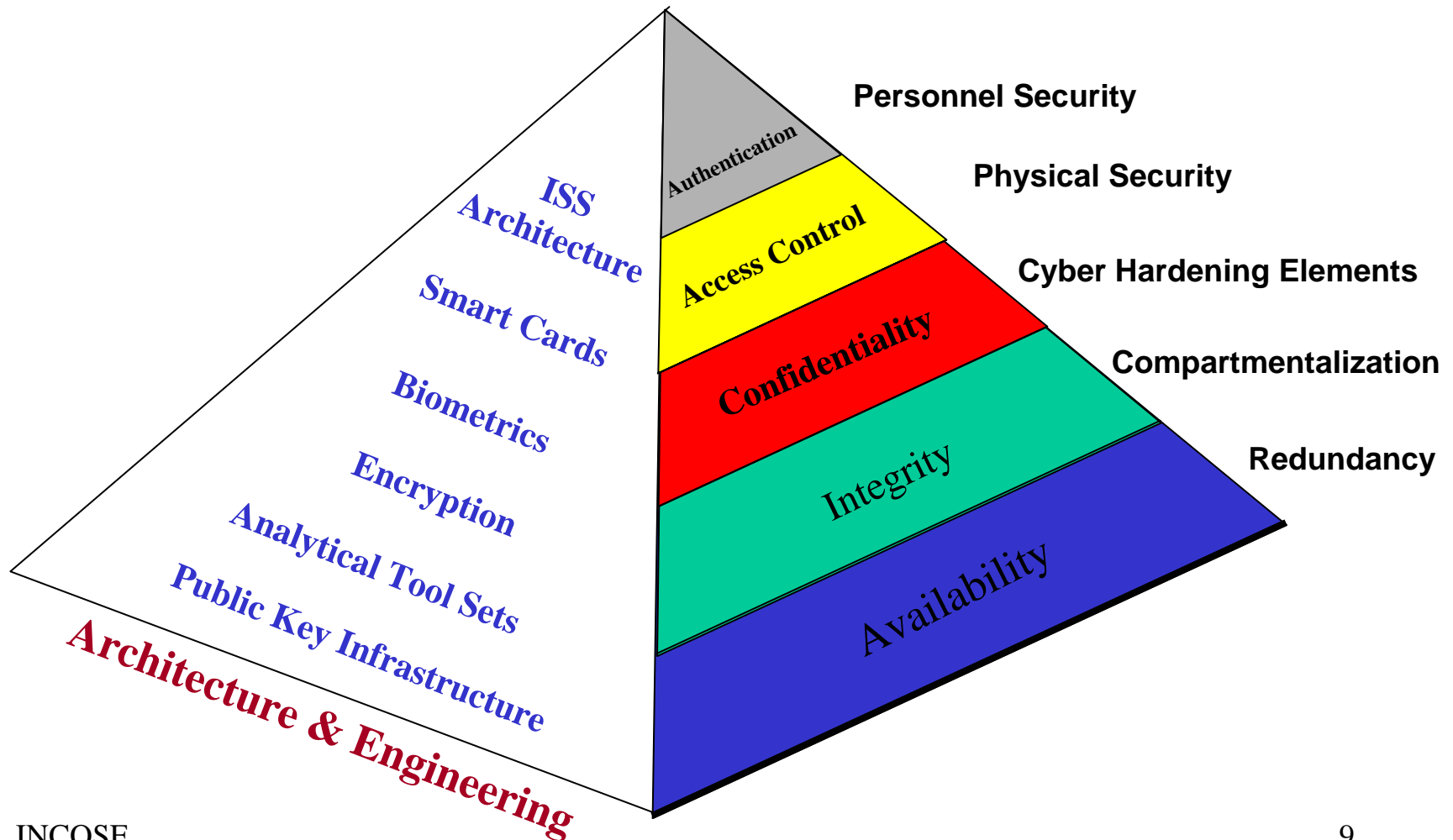


# *Awareness and Execution Actions*





# *Architecture & Engineering Perspective*





# *Architecture & Engineering Actions*

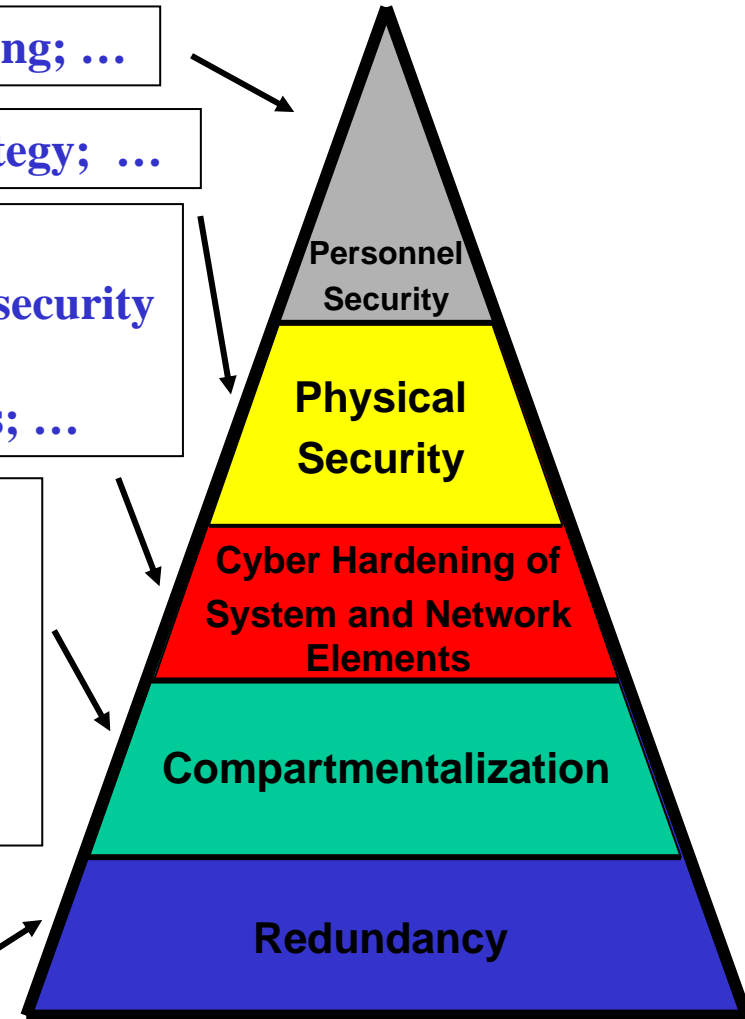
Create specialized FAA training; ...

Define smart card architecture and deployment strategy; ...

Allocate ISS requirements to each element; develop Common Criteria templates; tailor NIACAP; infuse security engineers into projects; define enterprise-wide PKI architecture; integrate safety and security techniques; ...

Define multiple domains with different security policies; define standards for VPNs, firewalls, etc.; research how to reduce data volume from intrusion detection; find ways to non-intrusively, continuously test network for policy compliance; develop analytic tools; operate test lab for new technologies; ...

Rely on fact that system is already engineered to accommodate occasional component failure





# *Conclusion*

- Because of the size and complexity of the Air Traffic Control System, only a systems approach can provide adequate defense
- The fundamental strategy guiding cyber defense is:
  - Harden individual system and network elements
  - Isolate elements to avoid “viral” spread
  - Back up elements to avoid service disruption
- Our systems approach implements this strategy