

# Federal Aviation Administration

## *Designing and Implementing A Cyber Security Defense*

**COMNET Conference**  
**January 28, 2003**

**Dan Mehan, PhD**  
*Assistant Administrator for  
Information Services and Chief  
Information Officer*



# *FAA's Cyber Security Liftoff*

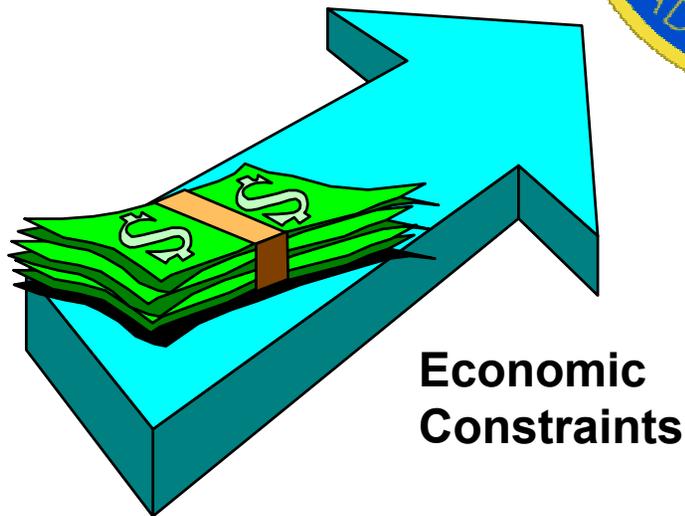
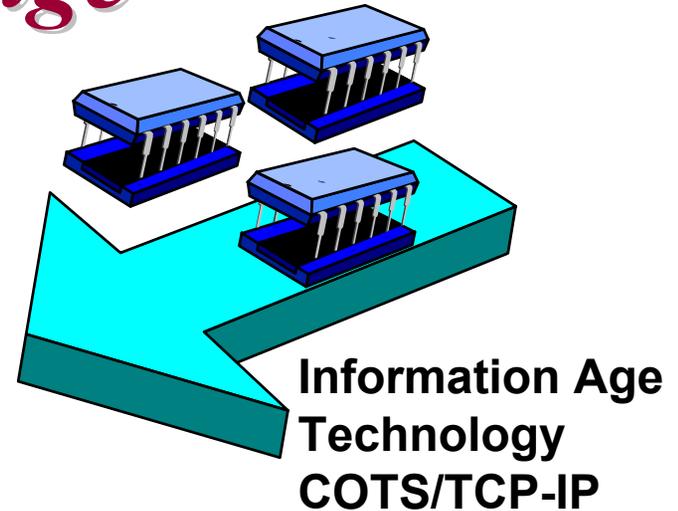
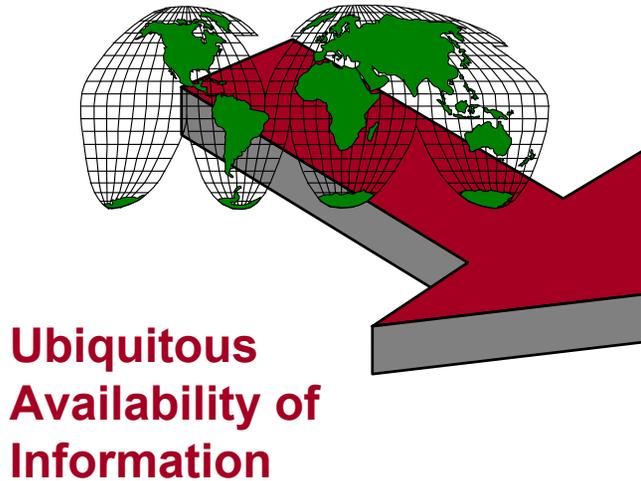
*Extended Frontiers*

*Systems Approach*

*Multiple Layered Protection*

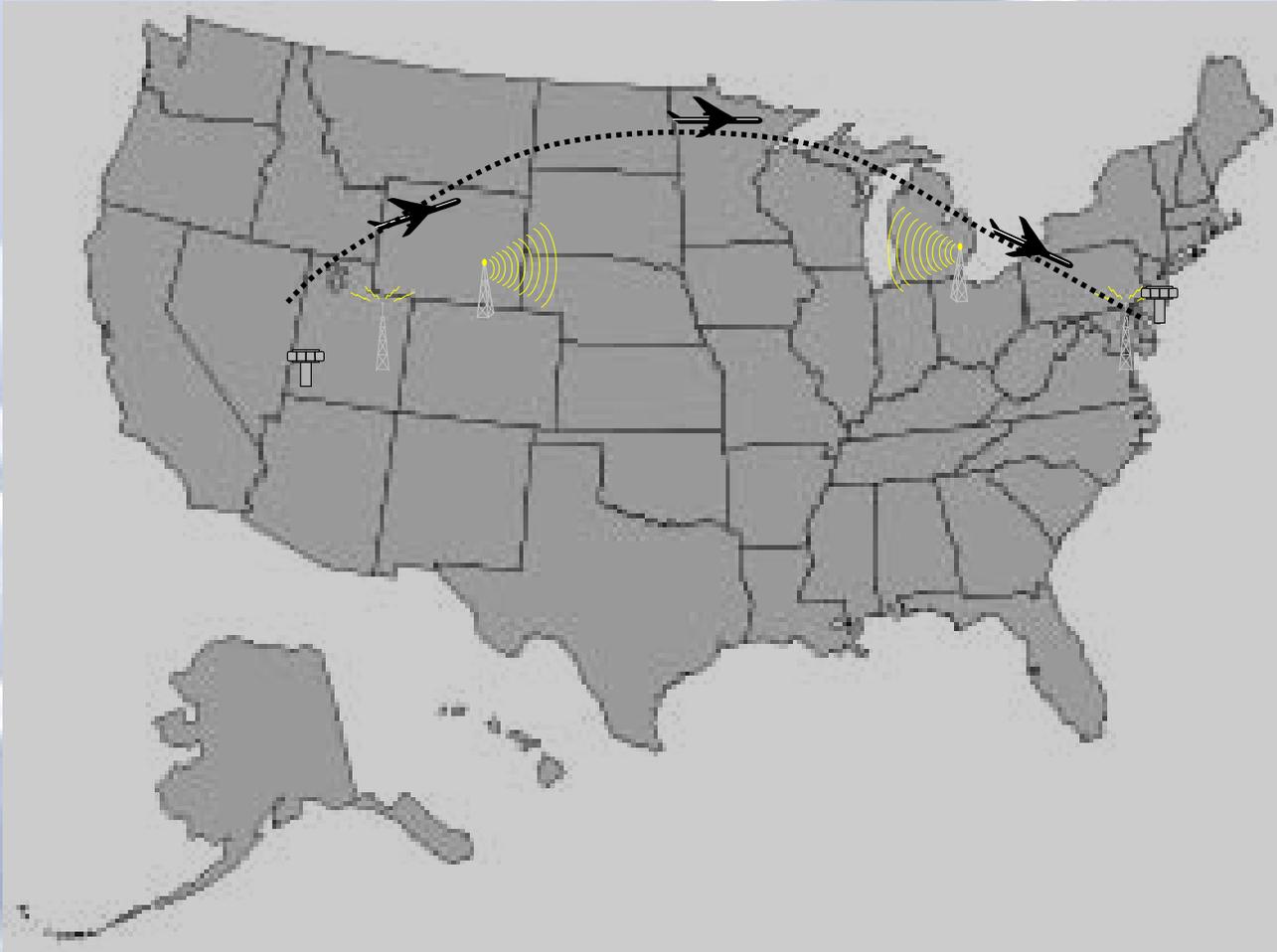
*Forces of Change*

# *Forces of Change*



# *FAA's Job*

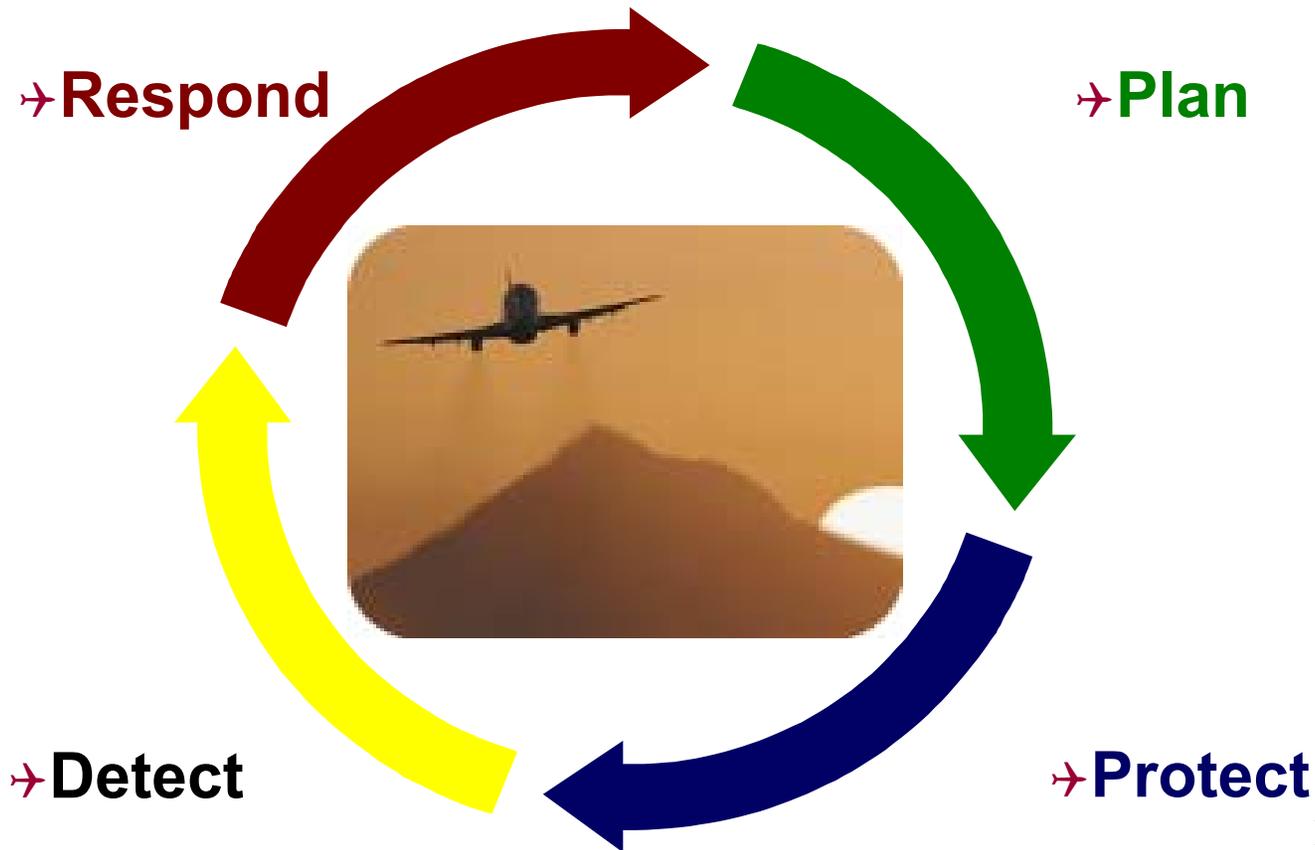
- **Manage 35,000 commercial flights to move 2,000,000 passengers safely each day**
- **Support more than 35,000 general aviation flights on a daily basis**
- **Regulate and certify the people and aircraft that use our airspace**



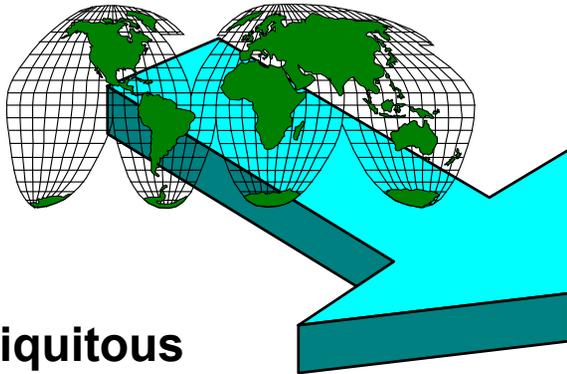
- **~ 500 FAA Managed Air Traffic Control Towers**
- **~ 180 Terminal Radar Control Centers**
- **20 Enroute Centers**
- **~ 60 Flight Service Stations**
- **~ 40,000 Radars, NAVAIDs, Radios, etc.**

# *CIO's Cyber Security Mission*

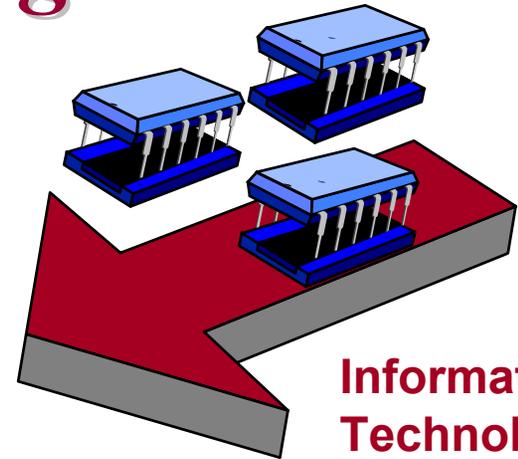
*Protect the FAA's information infrastructure and help the aviation industry reduce security risks through leadership in innovative information assurance initiatives*



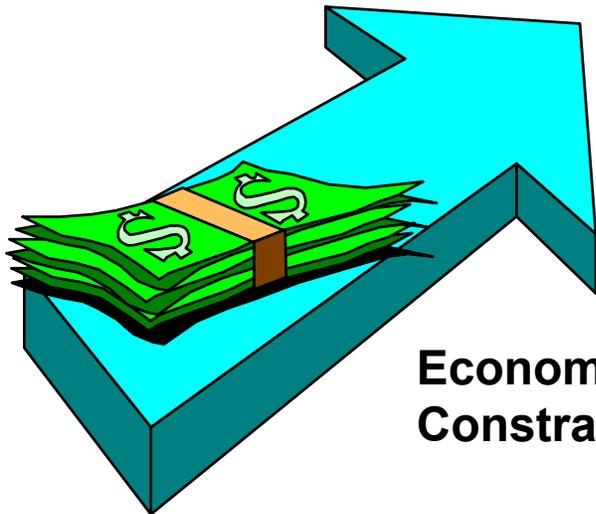
# *Forces of Change*



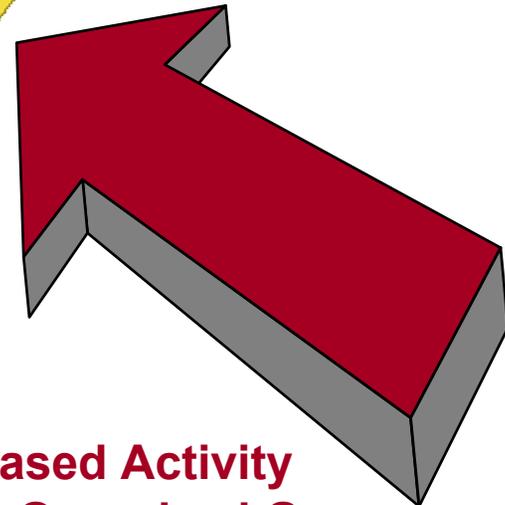
**Ubiquitous  
Availability of  
Information**



**Information Age  
Technology  
COTS/TCP-IP**

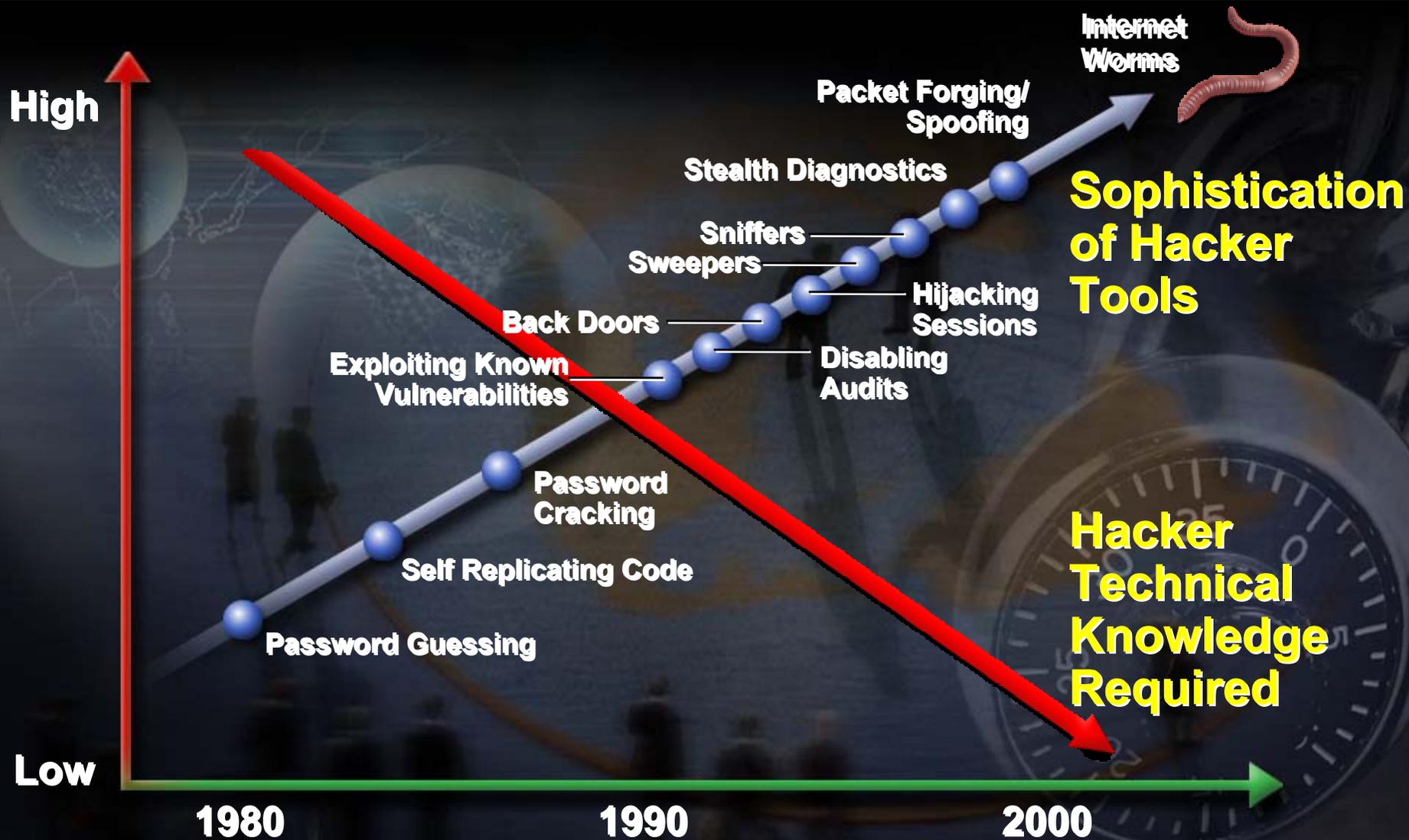


**Economic  
Constraints**

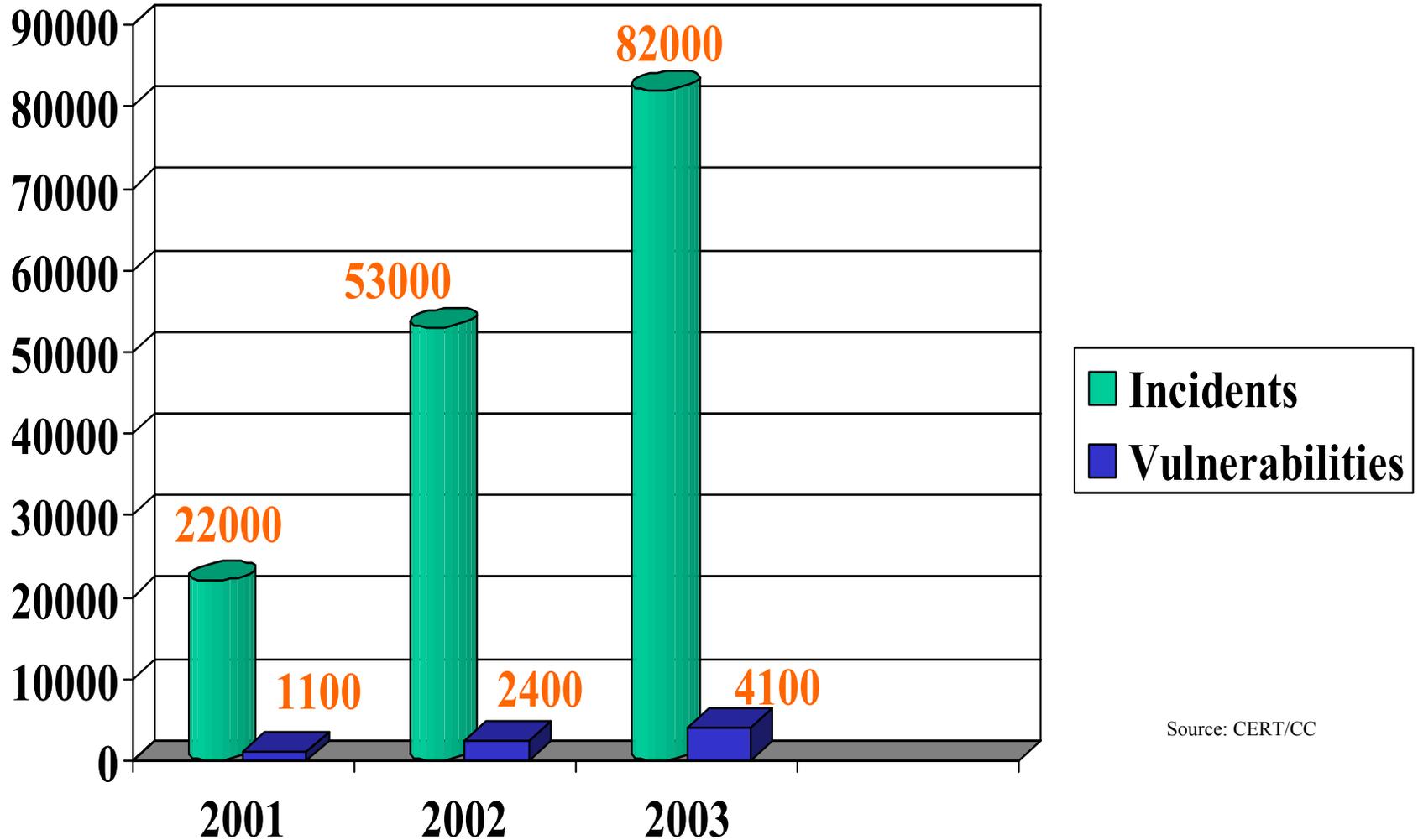


**Increased Activity  
From Organized Groups  
And Nation States**

# *Security and the Evolving Threats*

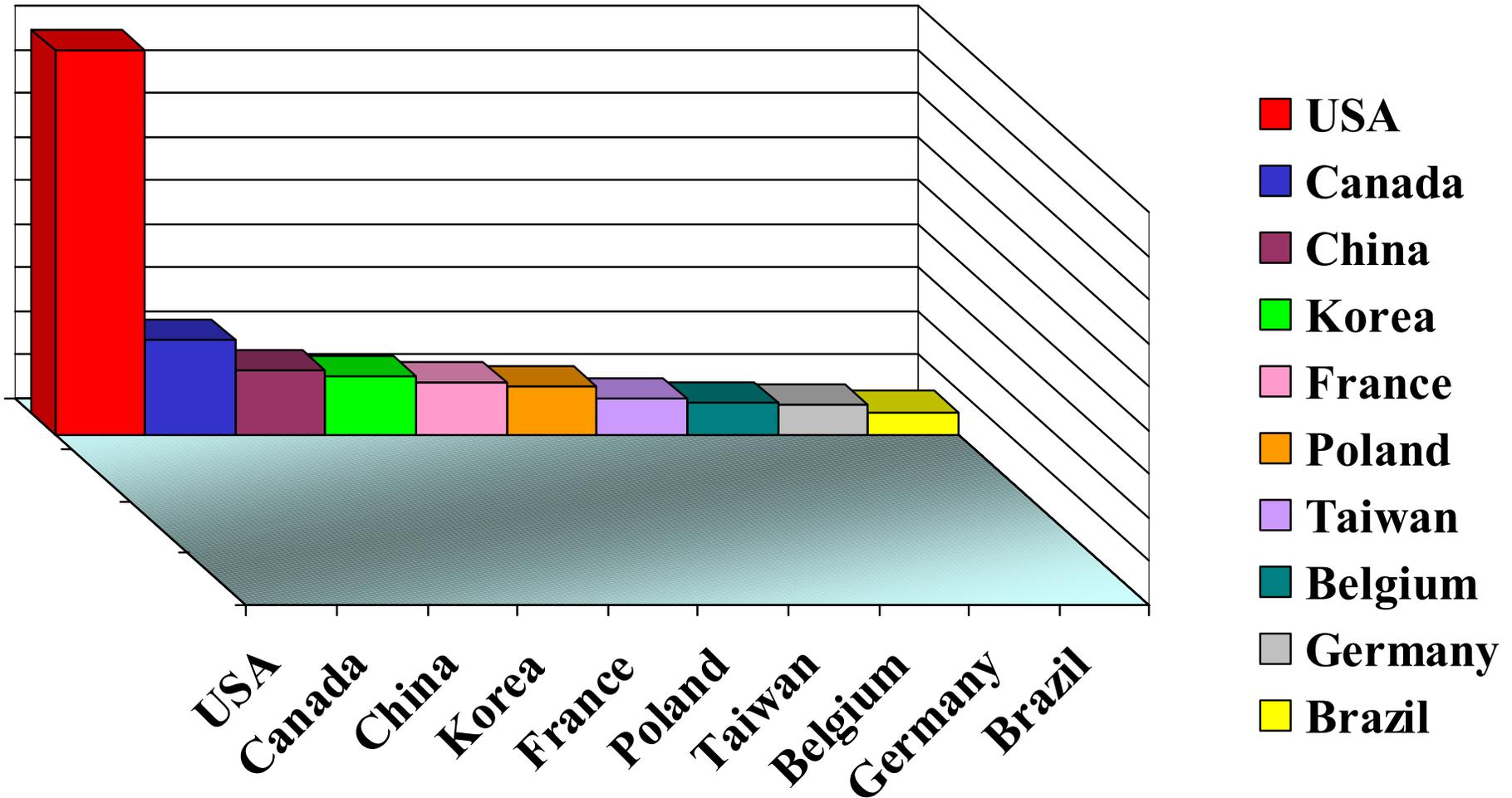


# *Incidents Reported*

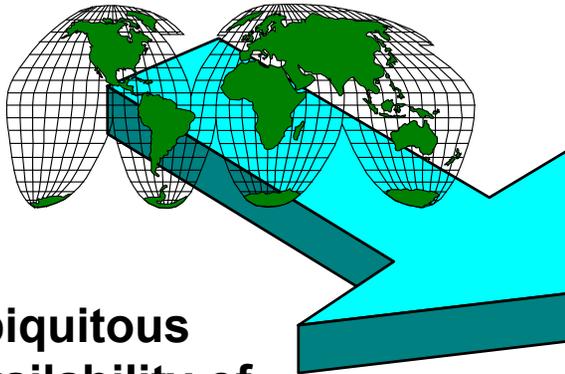


Source: CERT/CC

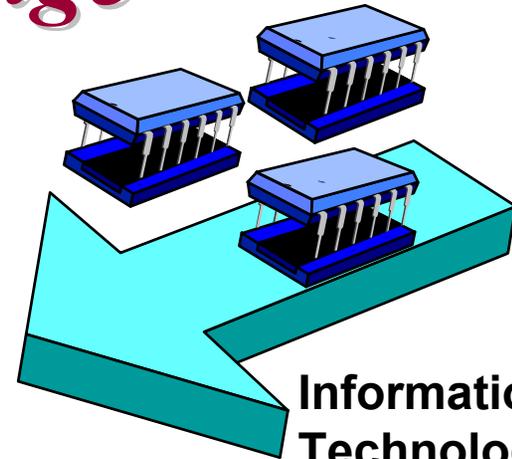
# *CSIRC Anomalous Traffic*



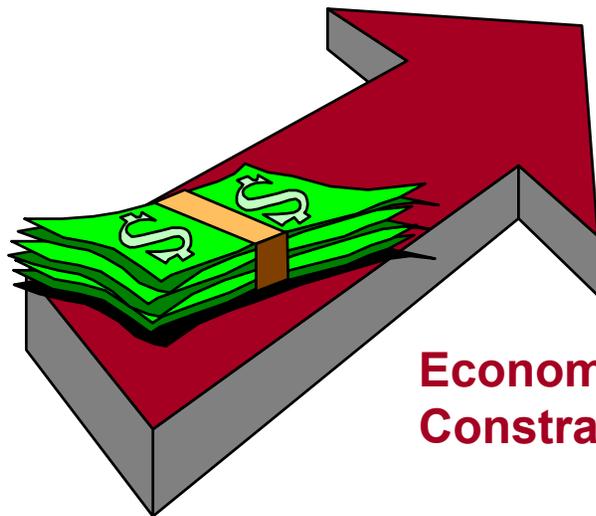
# *Forces of Change*



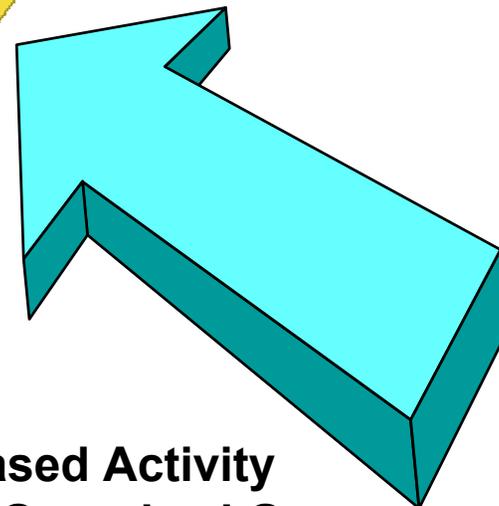
**Ubiquitous  
Availability of  
Information**



**Information Age  
Technology  
COTS/TCP-IP**

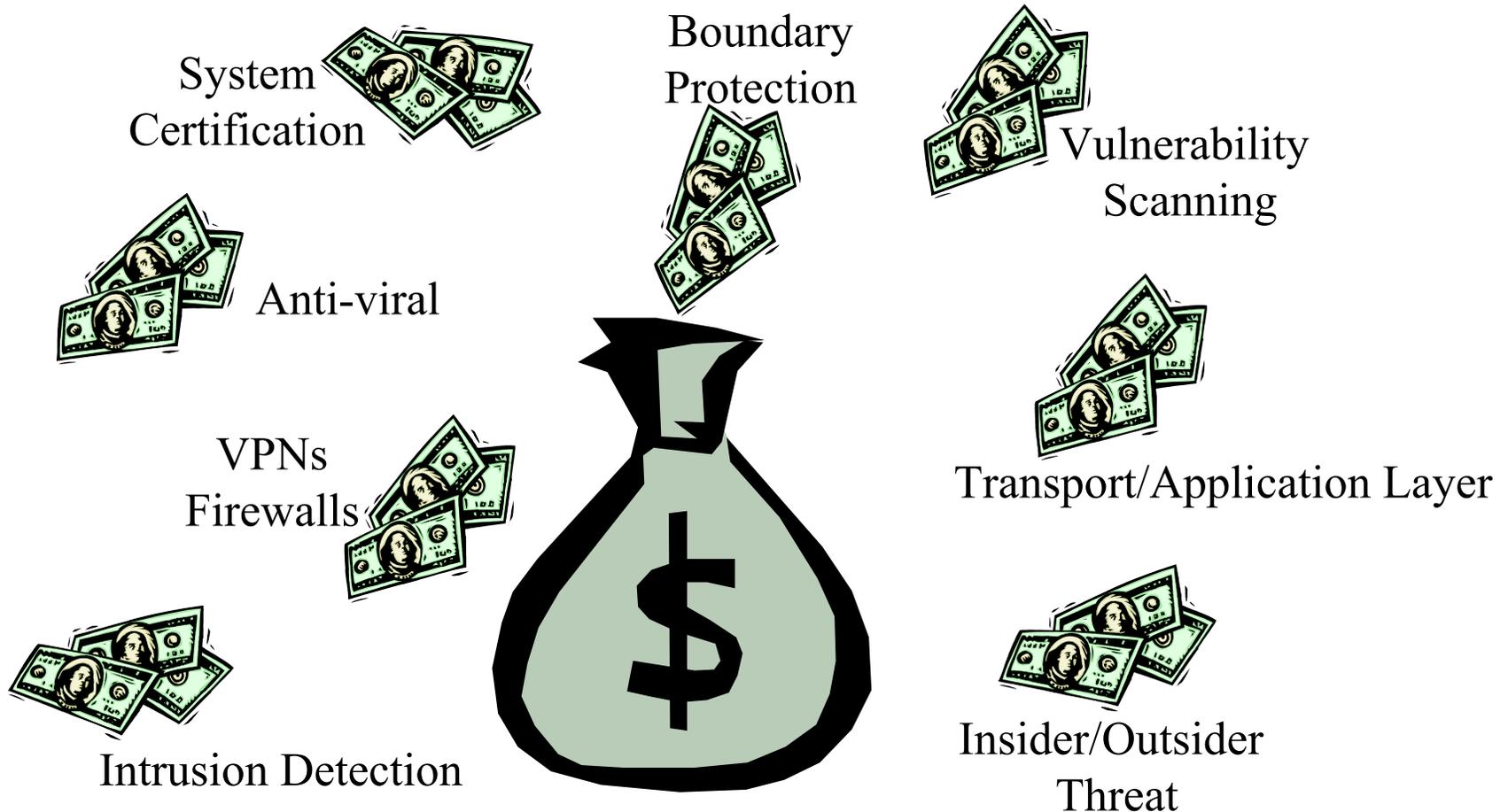


**Economic  
Constraints**



**Increased Activity  
From Organized Groups  
And Nation States**

# How to Invest Scarce Resources



# *FAA's Cyber Security Liftoff*



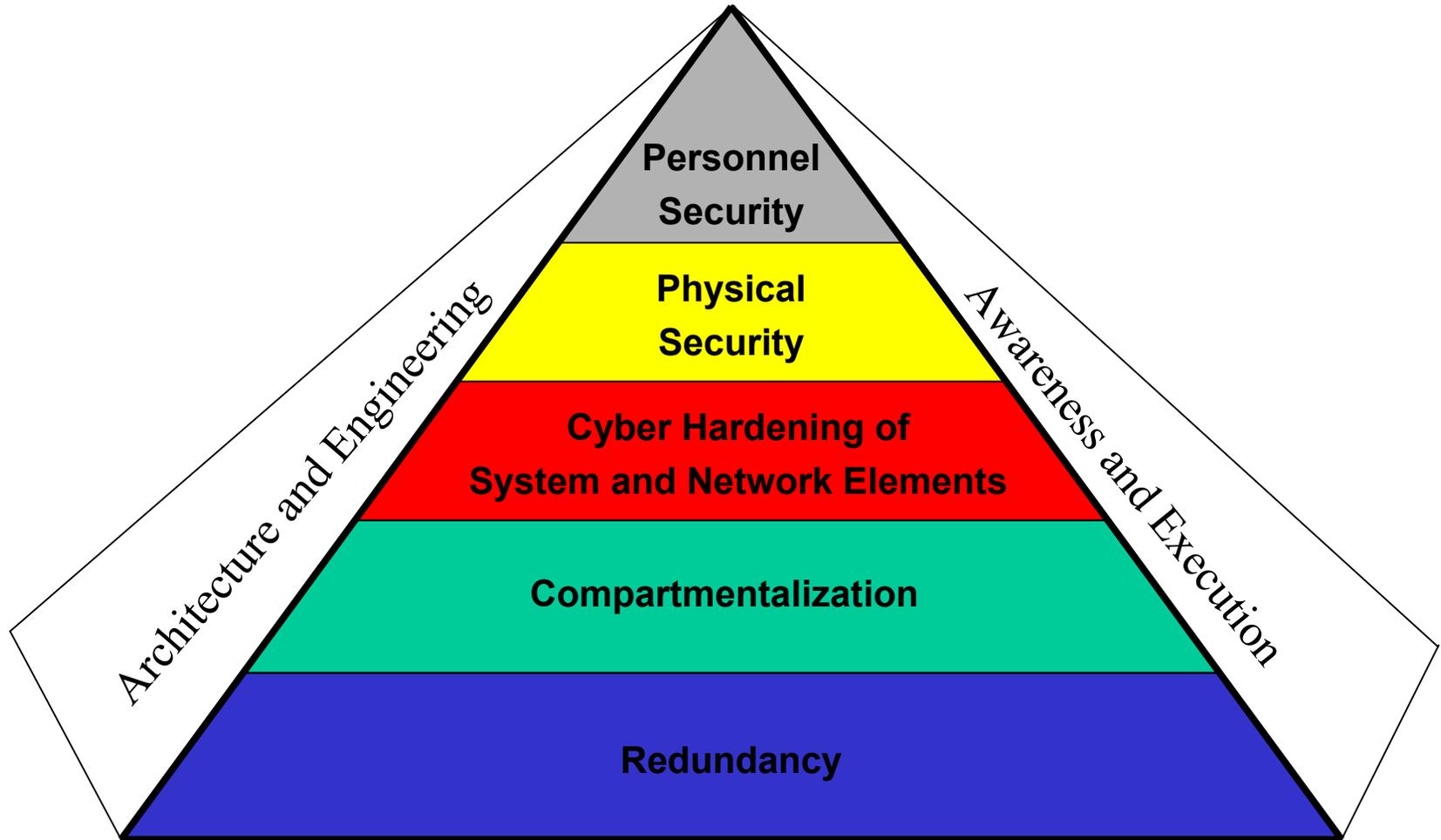
*Extended Frontiers*

*Systems Approach*

*Multiple Layered Protection*

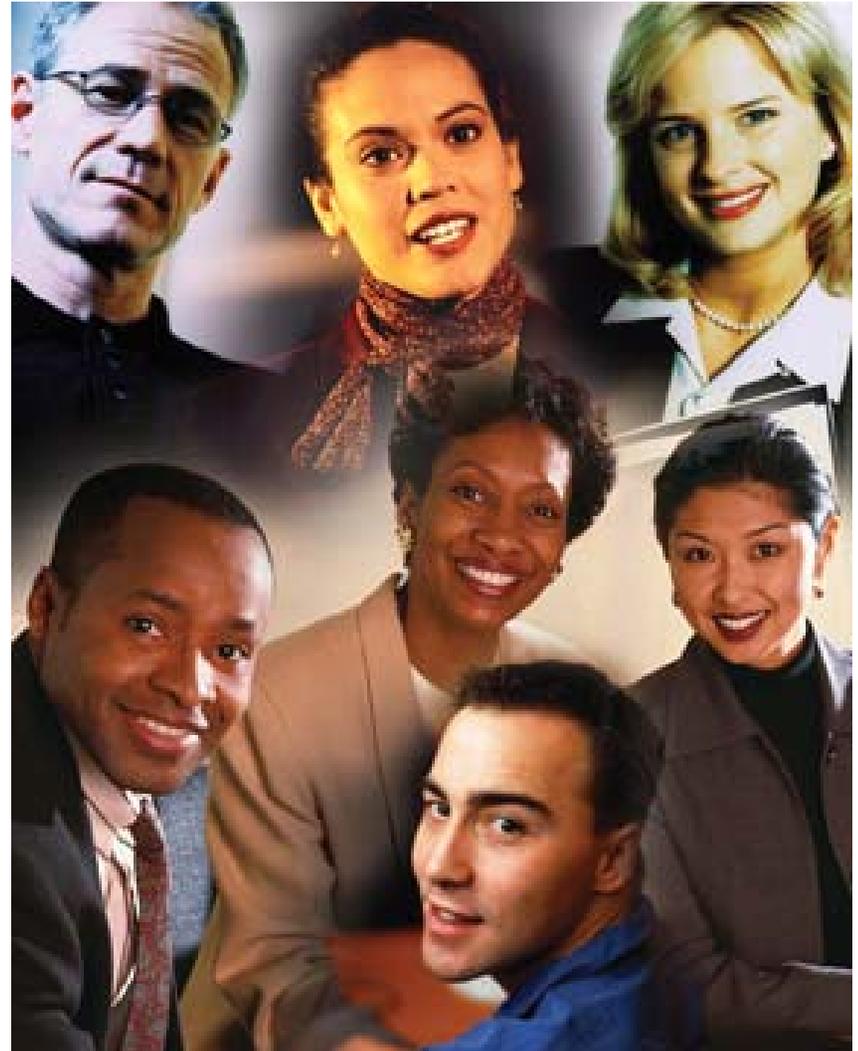
*Forces of Change*

# *FAA's 5 Layers Of System Protection*



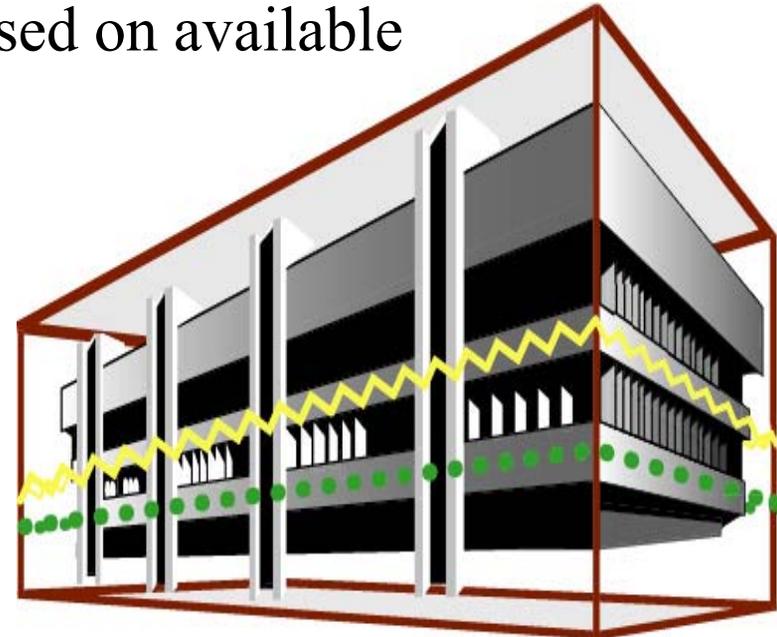
# *Personnel Security*

- IT security requirements are programmed into agency contracts
- Background checks are performed on Federal employees and contractors based on the sensitivity of their position
- Processes are being automated to improve efficiency and to facilitate cross-checking of databases



# *Physical Security*

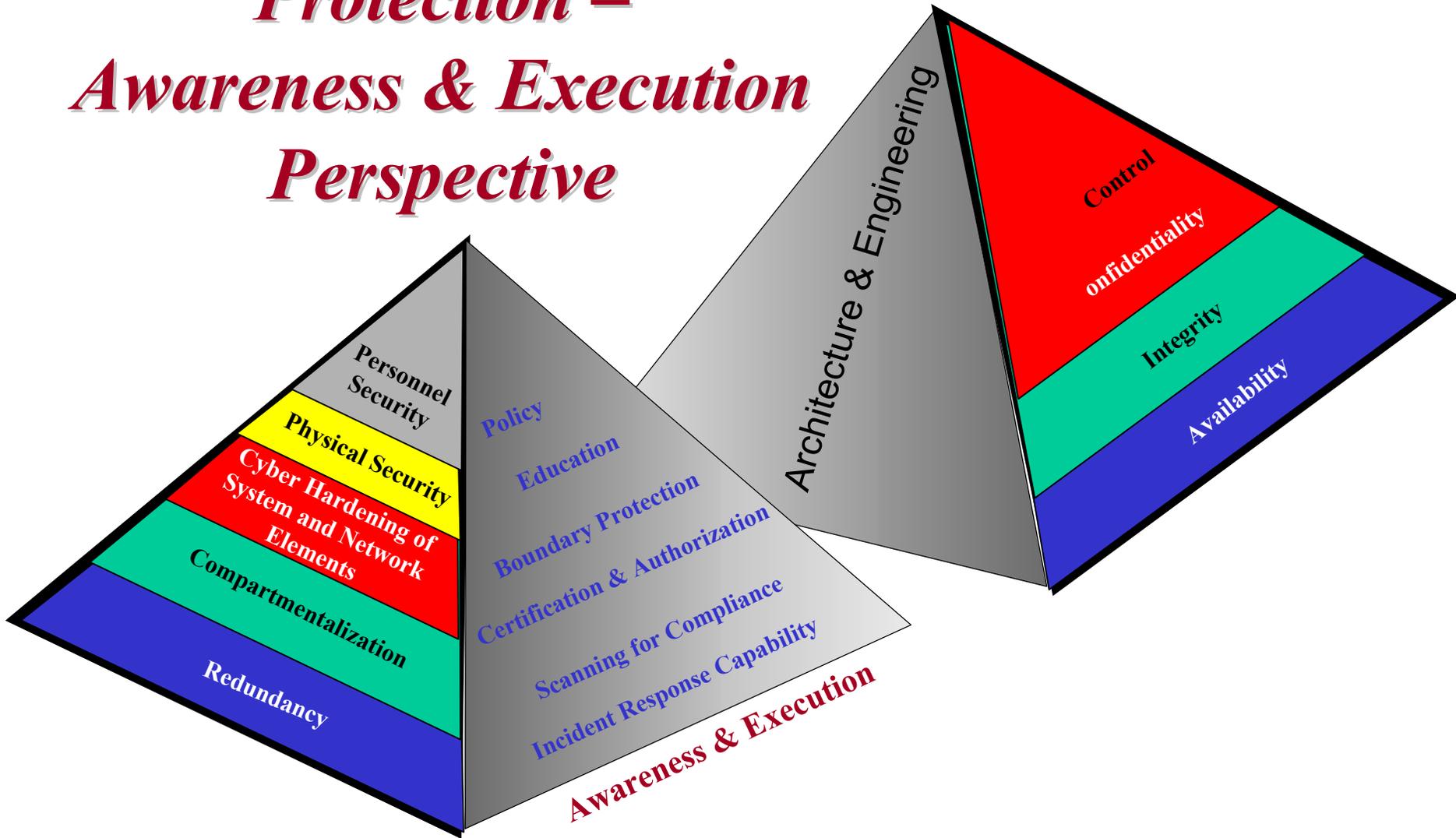
- FAA is in the process of upgrading and accrediting facilities to conform with post Oklahoma City enhanced security protection requirements
- Air traffic control facilities have been upgraded first, with enhanced access control and guard services at all major centers
- Phased approach will be used to complete appropriate level of upgrade at all facilities based on available technology and funding



# *FAA's Cyber Defense Strategy*

- Harden individual system and network elements
  - Make it difficult to knock out any single element
- Isolate elements to avoid “viral” spread
  - Create firebreaks to contain spread of detected attacks
- Back up elements to avoid service disruption
  - Augment incident recovery procedures to encompass potential cyber events

# *FAA's 5 Layers of System Protection – Awareness & Execution Perspective*



# *Policy & Education*

## **Policies are in place to address:**

Facility Security Management  
Personnel Security Program  
Information Systems Security  
Internet Access Points and Internet Services  
Software Release

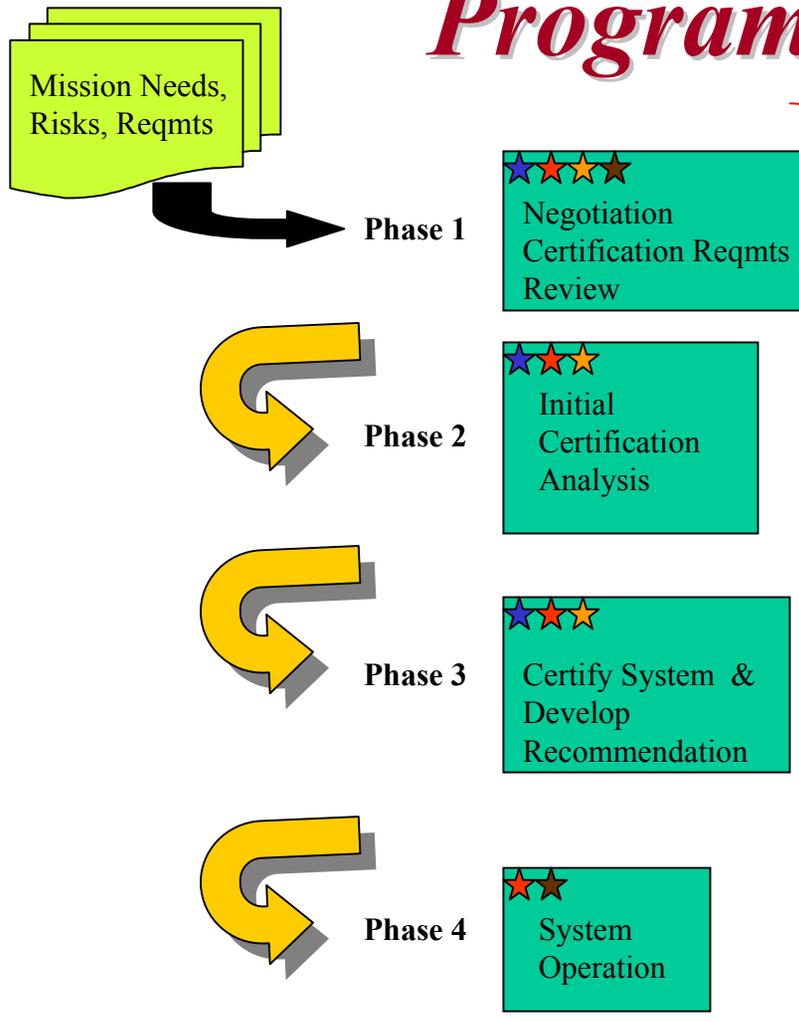
## **Active Training Program:**

- **FY-00** – Over 40,000 employees viewed 30 minute training video on awareness. Also, 200 employees trained on vulnerability assessment.
- **FY-01** – More than 4,000 employees attended Awareness Day sessions held throughout the FAA. More than 100 employees attended CISSP Training.
- **FY-02** - Delivered Web-based awareness portal and computer-based training. Also deployed mobile training teams.
- **FY-03** – More than 600 key personnel being targeted for specialized training; follow up Awareness Days planned throughout the FAA; continued emphasis on IT curriculum at IRMC and on computer-based training.



# *National Information Assurance Certification and Accreditation Program (NIACAP)*

- ★ Developer
- ★ Operator
- ★ Certifier
- ★ User Rep

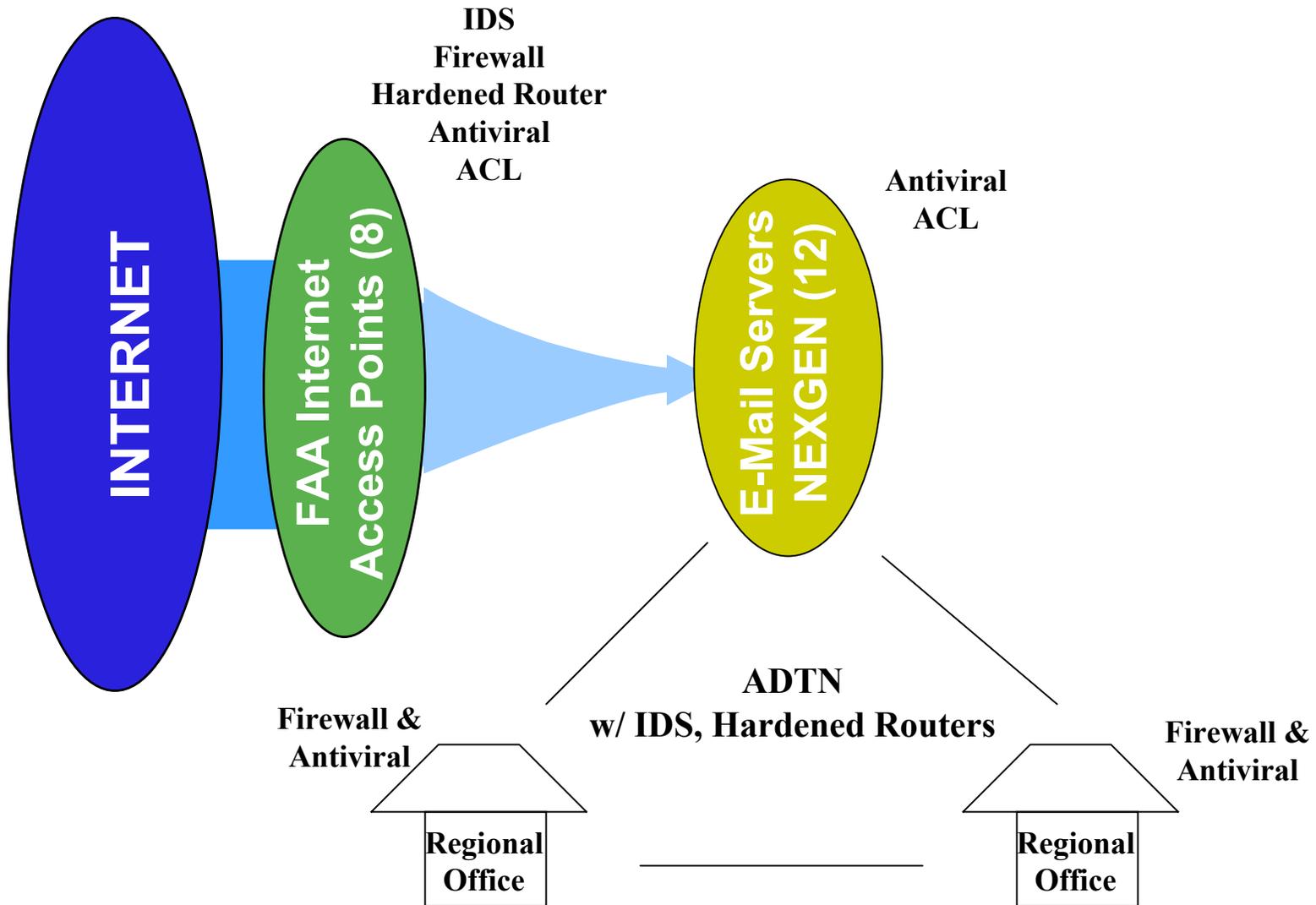


**Nationally Recognized Process**

**Security Requirements Review  
During Milestone Zero**

**Cradle to Grave Program**

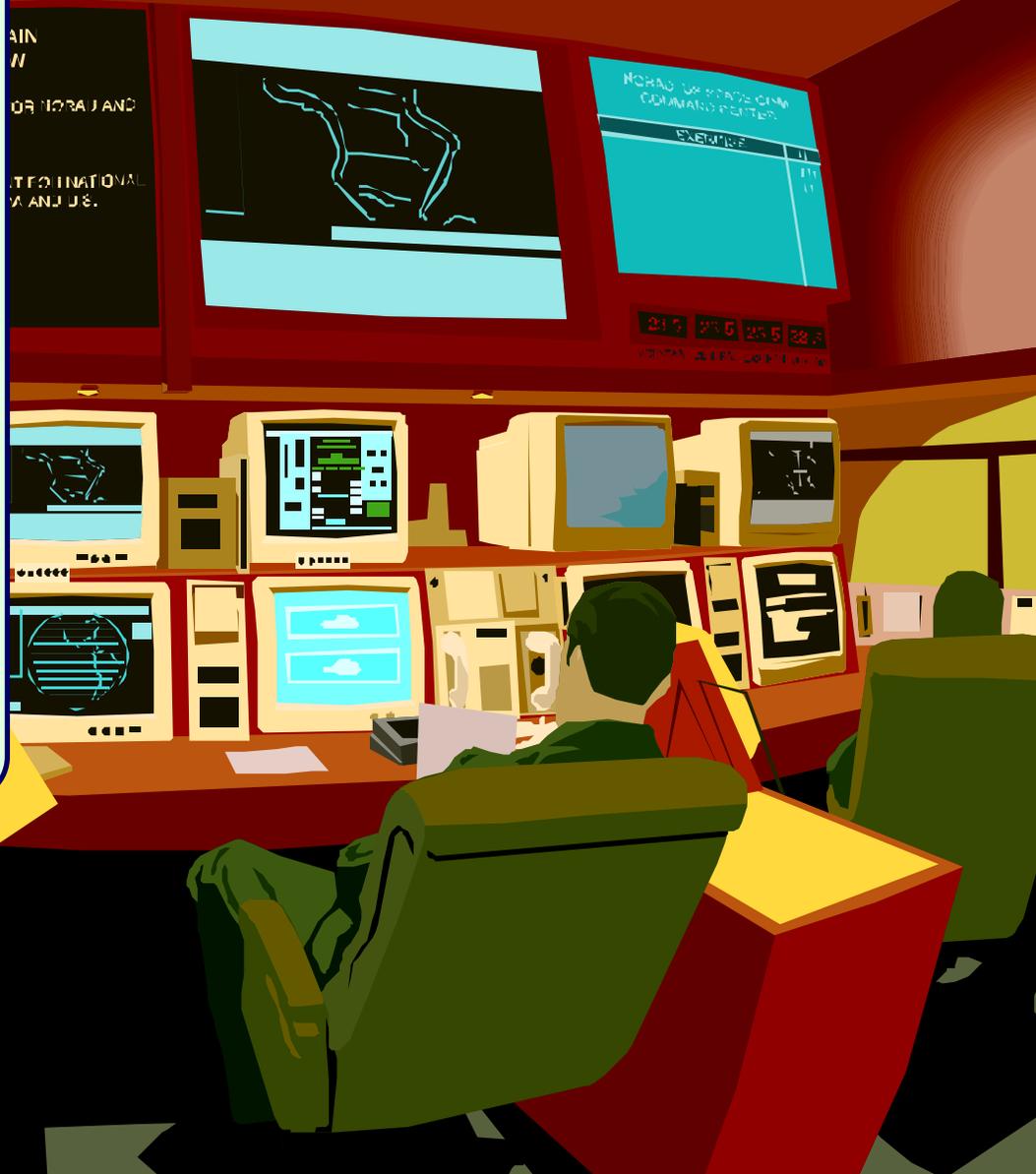
# *Boundary Protection*



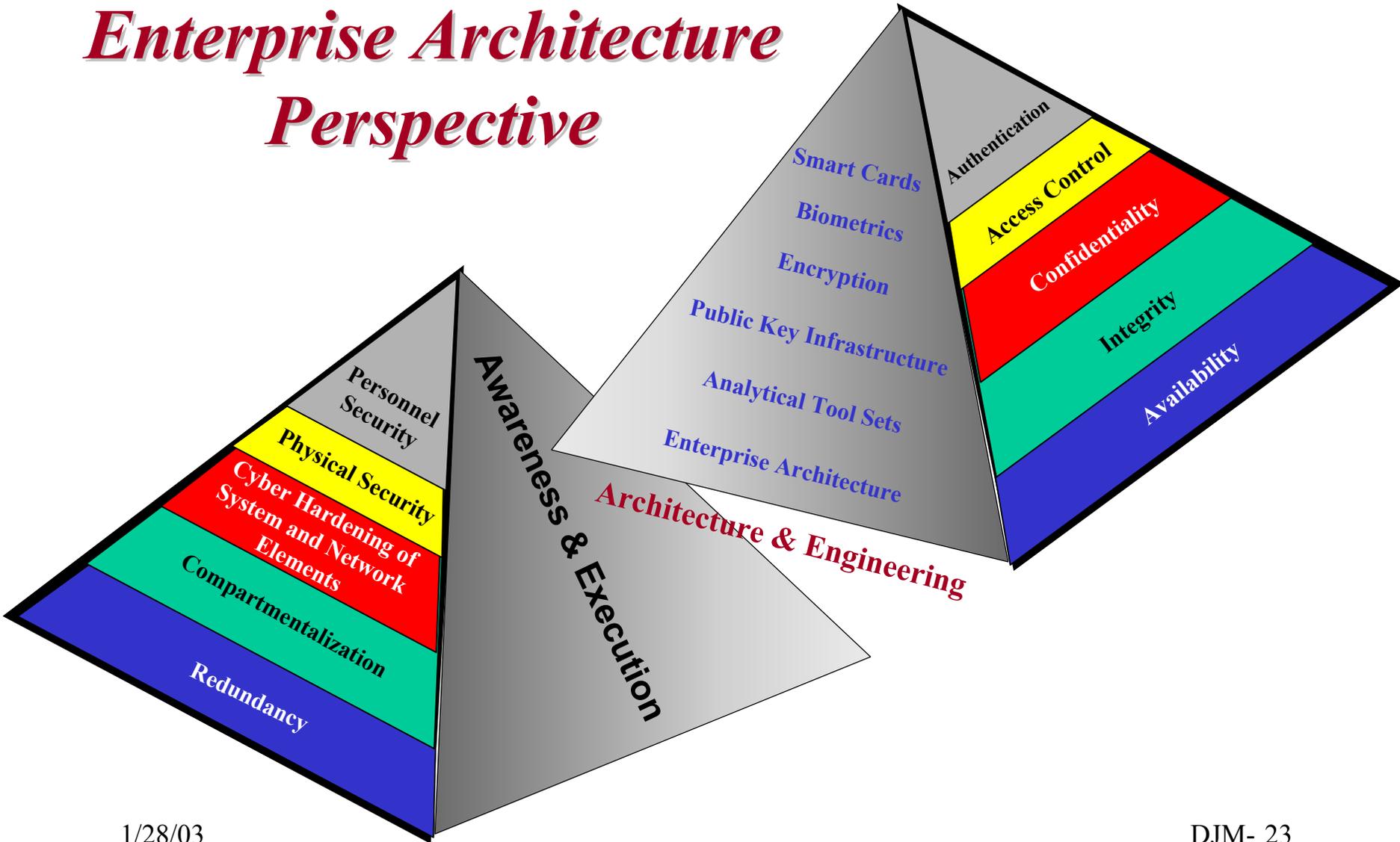
# *System Compliance Scanning Program*

- Scanning tools being tuned to “SANS Top 20” – 250 common vulnerability events
- 150 employees trained to conduct scanning
- Proactive testing for unremediated vulnerabilities
- Remediation progress being tracked with system administrators

# COMPUTER SECURITY INCIDENT RESPONSE CENTER (CSIRC)



# *FAA's 5 Layers of System Protection – Enterprise Architecture Perspective*



# *Planned FAA Smart Card Attributes*

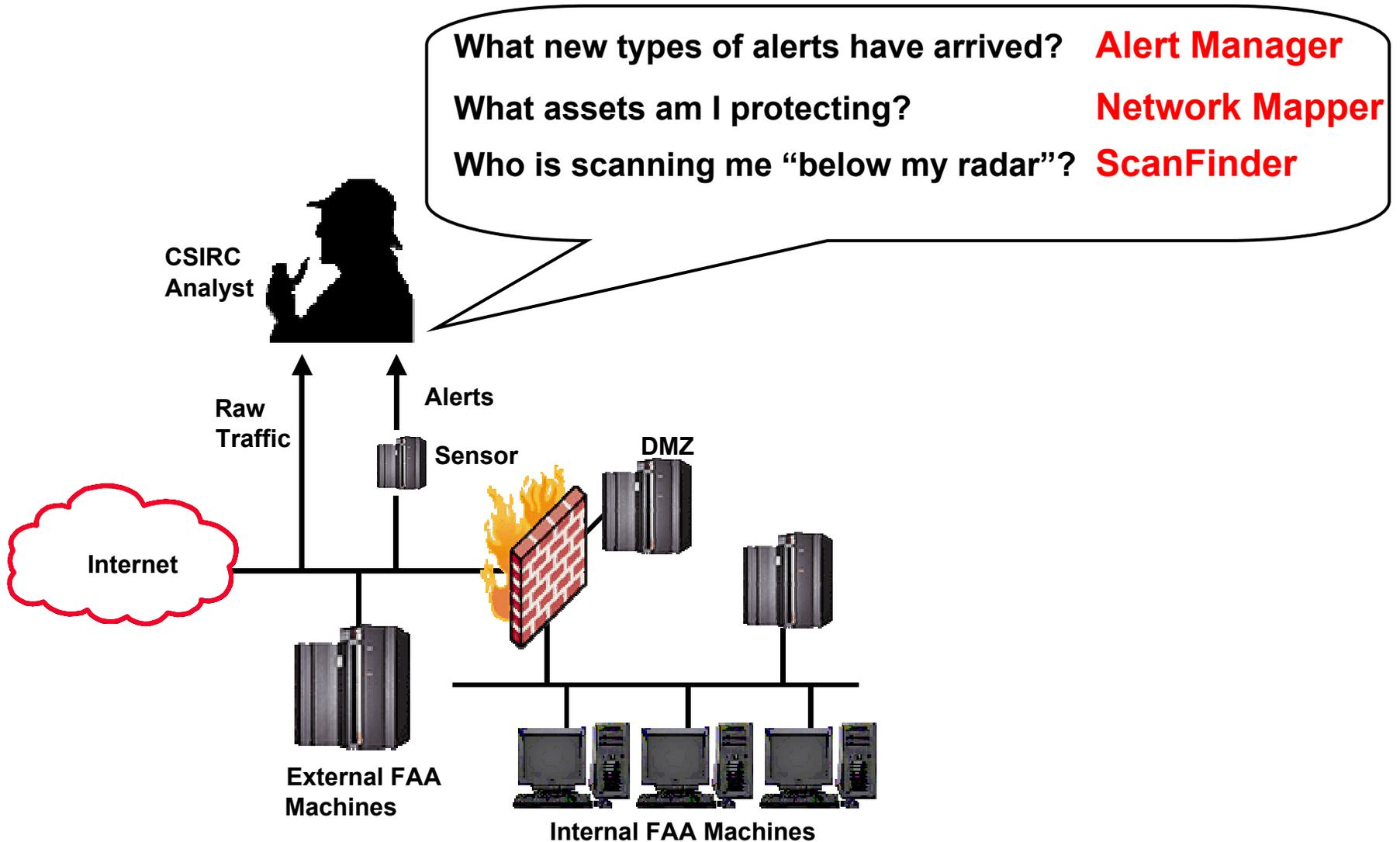
- Technology based on requirements to support both physical and logical access and backward compatibility
- The core technologies planned for the card platform:
  - Integrated Circuit Chip (ICC)
  - Contactless (Proximity) Chip
  - Photo Identification
  - Magnetic Stripe
  - Barcodes
- Placeholders on the ICC for:
  - Biometrics
  - PKI Certificates (Digital Signature, Encryption, Identity & Authentication)



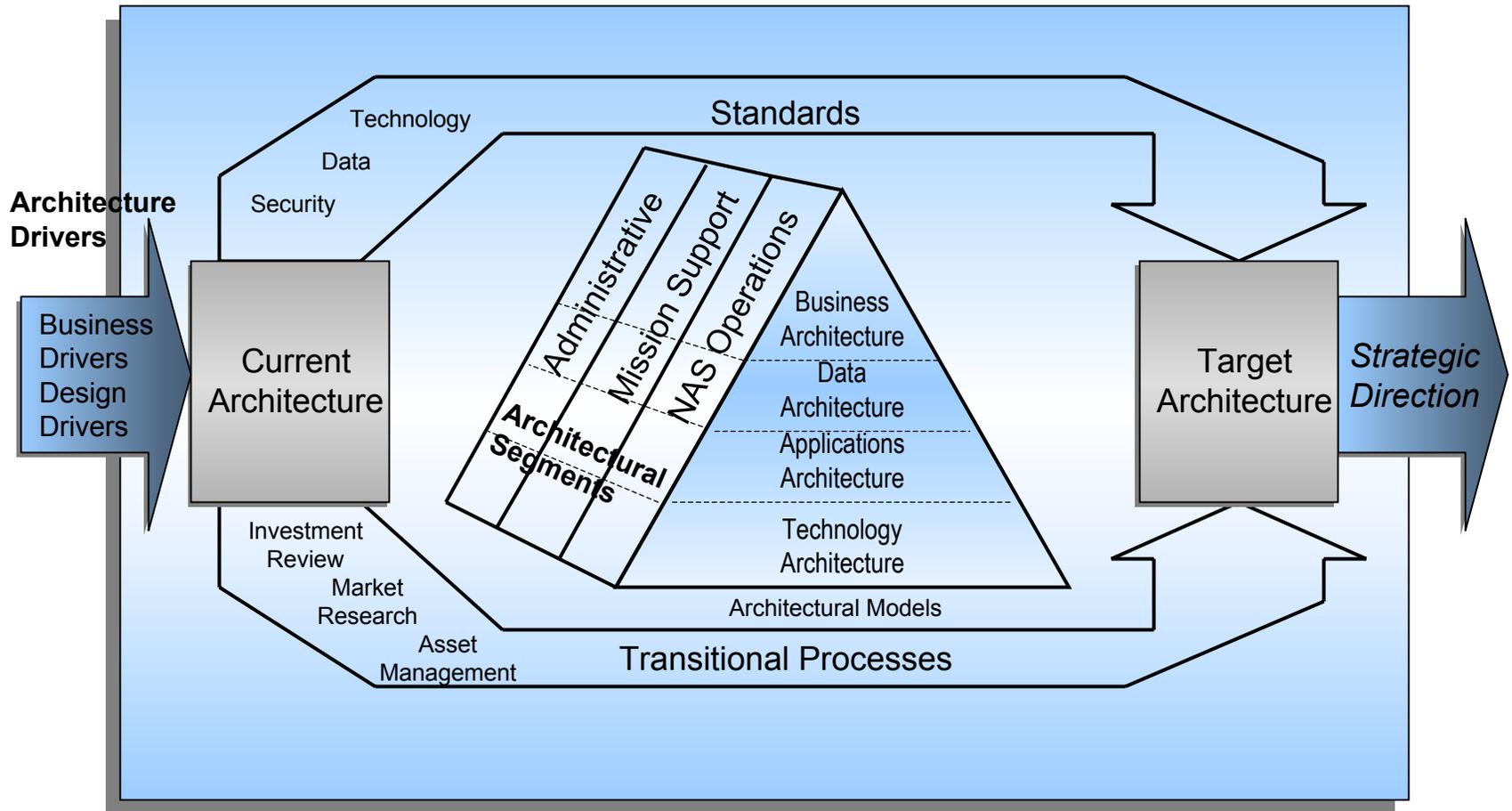
# *FAA Program for PKI*

- FAA PKI Steering Committee is developing architecture and standards for cross agency use
- Requirements for PKI will be based on applicable existing national and international standards
- Government Paperwork Elimination Act necessitates use of digital signature standards and business process reengineering
- Digital signature and encryption capabilities will be used to ensure confidentiality, data integrity, authentication, and non-repudiation.

# Mathematically-Based “Cool Tools”



# *Enterprise Architecture Framework*



# *FAA's Cyber Security Liftoff*



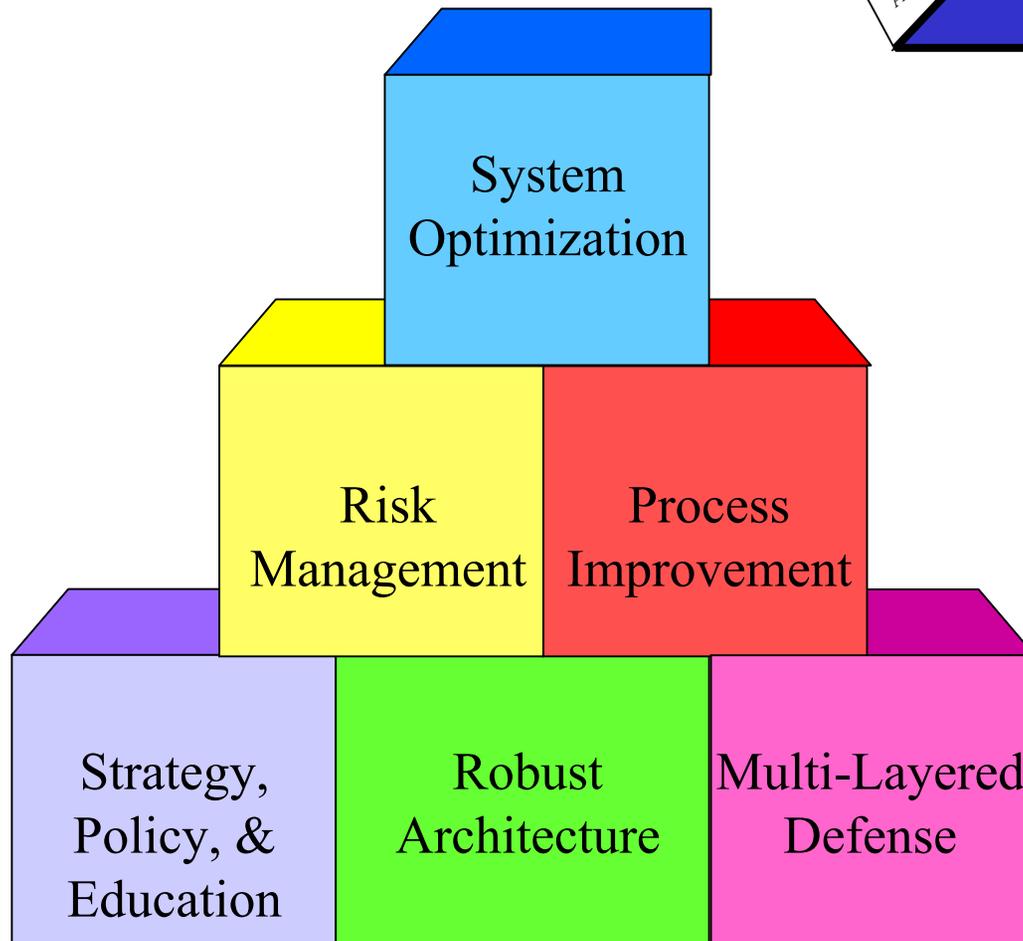
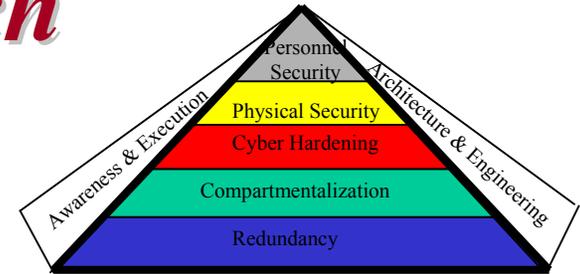
*Extended Frontiers*

*Systems Approach*

*Multiple Layered Protection*

*Forces of Change*

# *FAA's Systems Approach To Cyber Security*



# *Professional Development*

Continuous emphasis on training to evolve our employees

- Cyber Corps
- Computer Information Systems Security Professionals
- Specialized training with certifications for key personnel
- Continuing awareness events for all FAA personnel

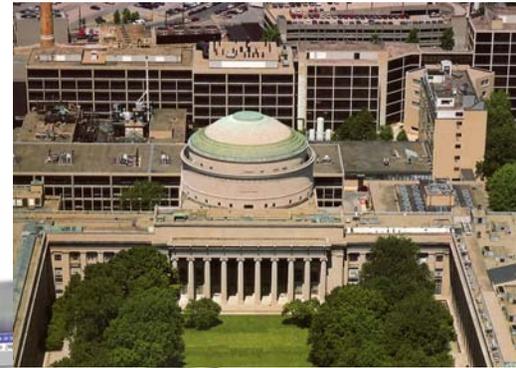


# *Extending the Frontiers*

## Private



## Universities



## Public



FedCIRC



NIPC



JTF-CNO 1/28/03



NSIRC



## International

# *FAA Cyber Security*

## *Key Concepts*

- A broad system approach must be used because of the size and complexity of the FAA information infrastructure
- A robust enterprise architecture with multiple layers of protection is a key to success
- Constant vigilance in terms of strategic planning, compliance monitoring, and intrusion detection is required
- People and processes must be married with technology and optimized for a successful program
- The challenge is pervasive and global and requires outreach to all segments of the nation's critical infrastructure, as well as to other nations