

Federal Aviation Administration

Paradigm Shifts, Paradoxes, and Prognostications

Adapted from Talks Given at:
IEEE Spring Conference, Boston, MA
ITAA Regional Meeting, Santa Clara, CA

Dan Mehan, Ph.D.

*Assistant Administrator for
Information Services and Chief
Information Officer*

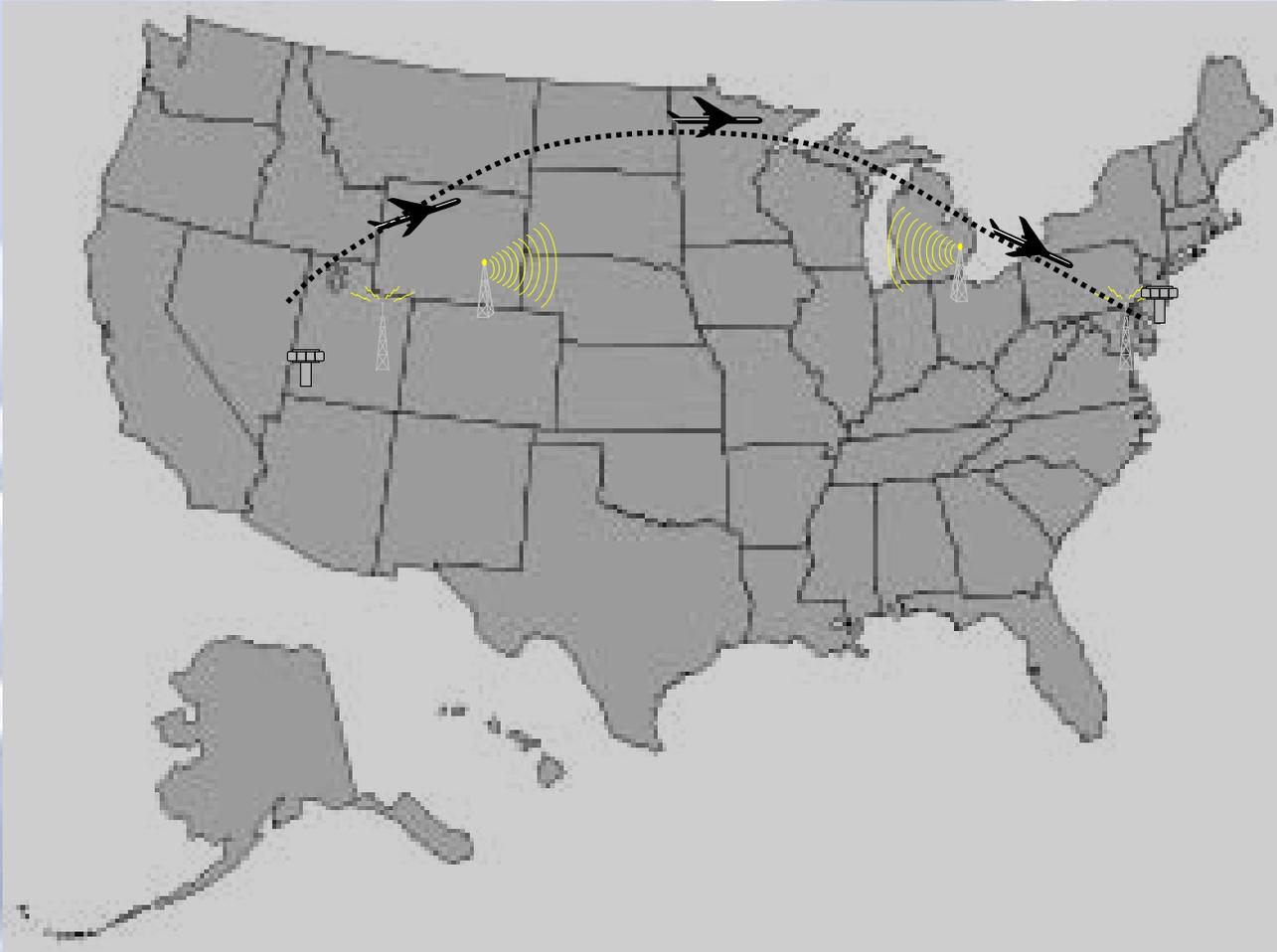


Paradigm Shifts, Paradoxes, and Prognostications

- **Harnessing the Infinite Resource**
- Defending in the Face of Increasing Propagation Speeds
- Securing the Whole Even When Parts Have Been Compromised
- Prioritizing Amidst a Plethora of Alternatives
- Extending the Frontiers

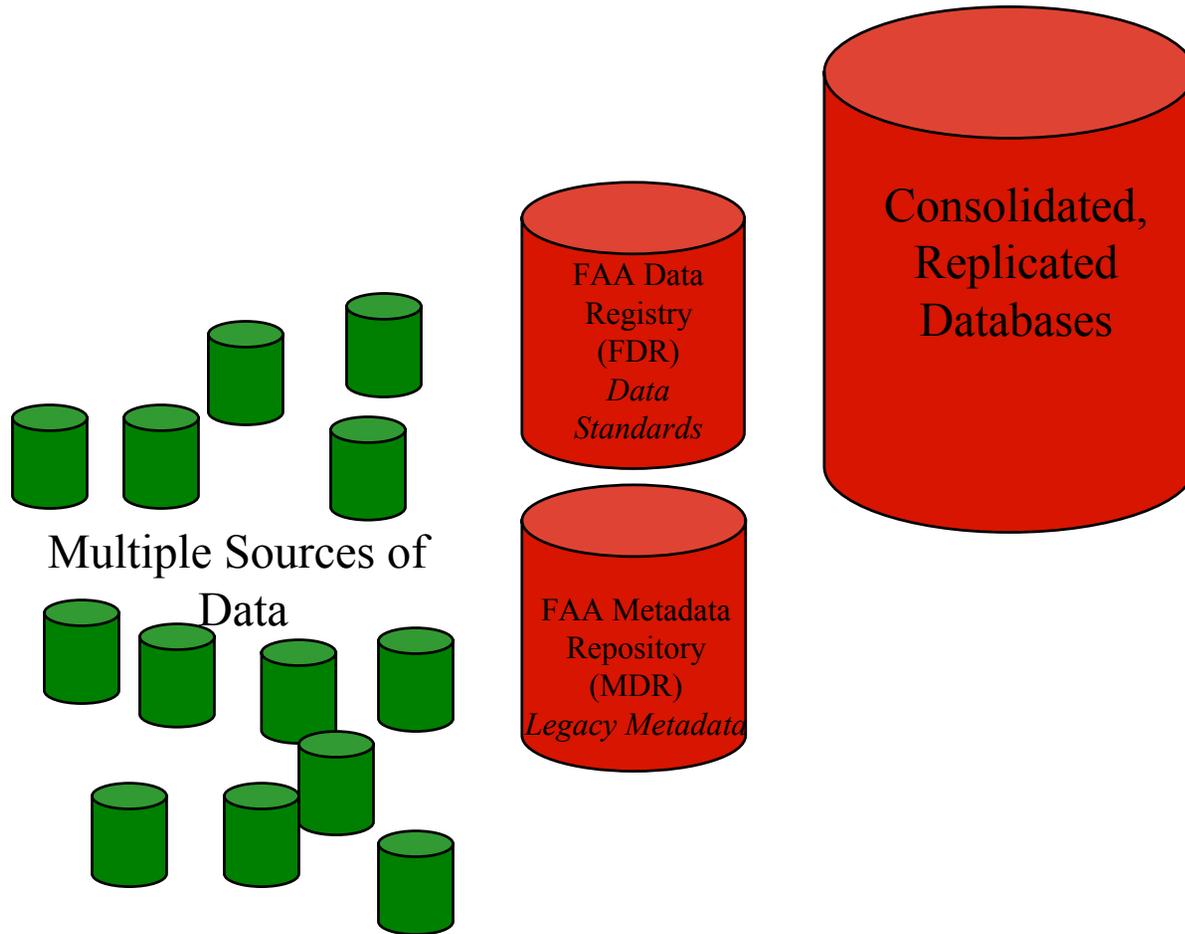
FAA's Job

- ➔ **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.**

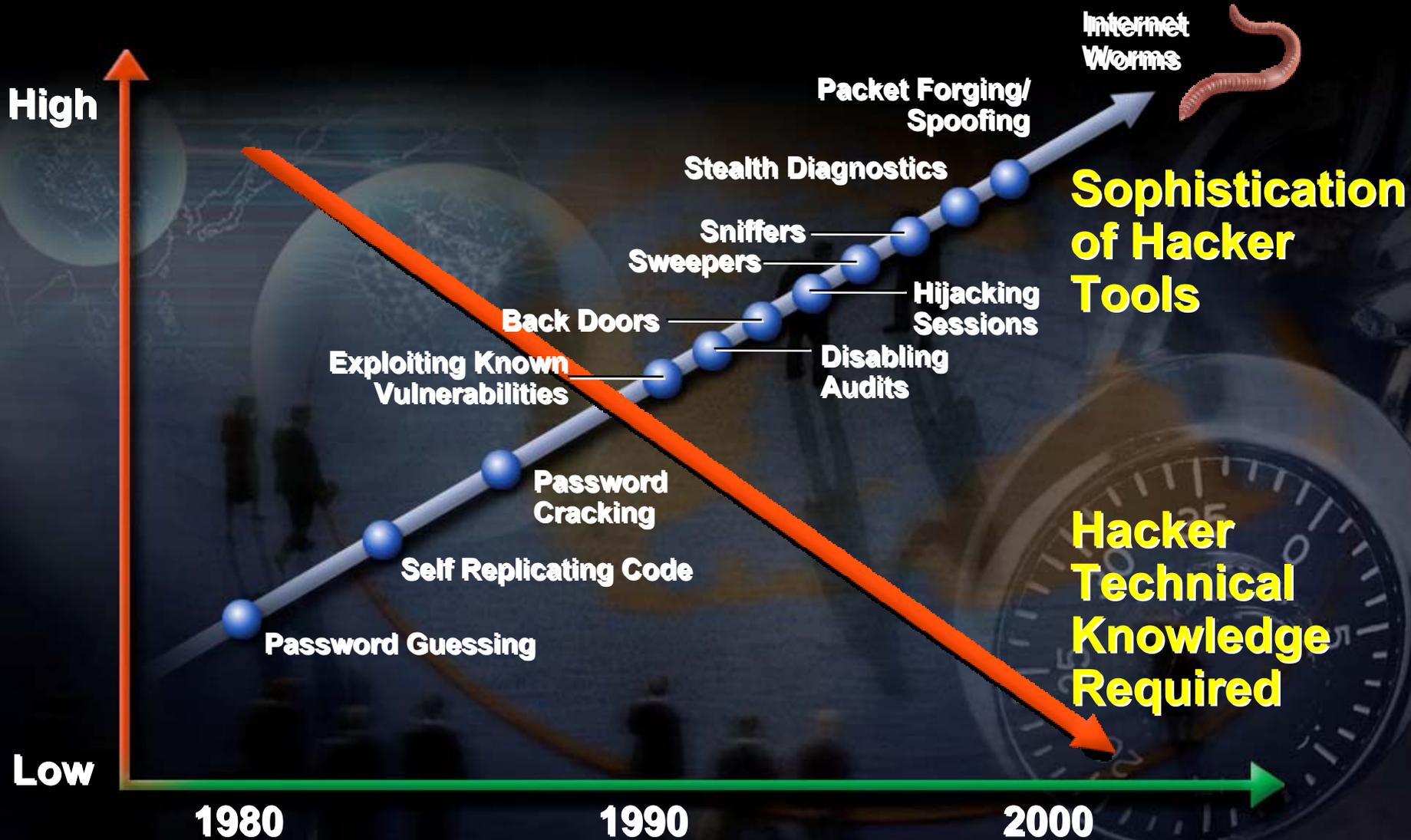
Database Evolution



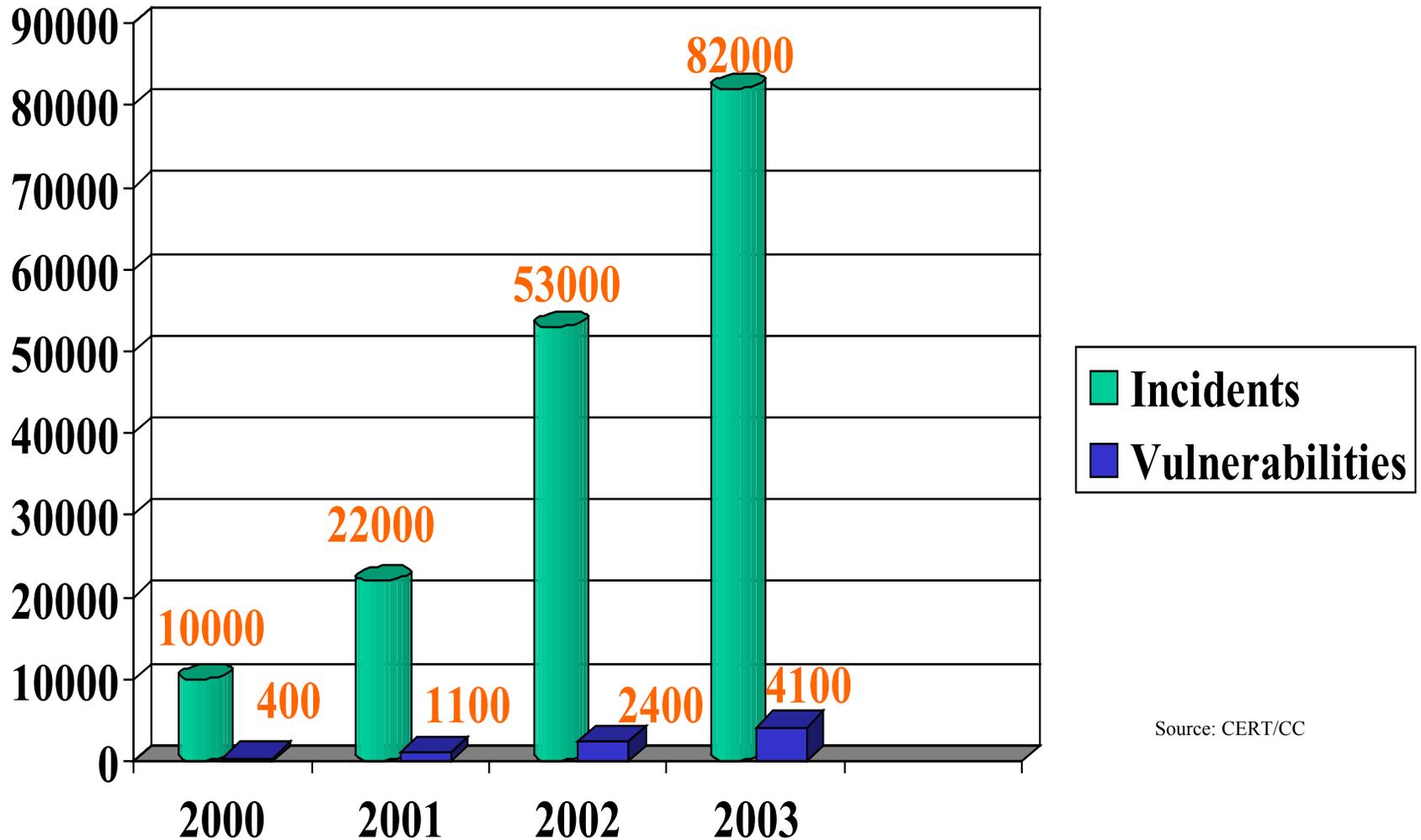
Paradigm Shifts, Paradoxes, and Prognostications

- Harnessing the Infinite Resource
- Defending in the Face of Increasing Propagation Speeds
- Securing the Whole Even When Parts Have Been Compromised
- Prioritizing Amidst a Plethora of Alternatives
- Extending the Frontiers

Security and the Evolving Threats



CERT Incidents Reported



Source: CERT/CC

Rapidly Decreasing Time for Worms to Spread

Infected Population Doubling Time

Code Red 37 minutes

Slammer 8.5 seconds



Vulnerable Population Saturation Time

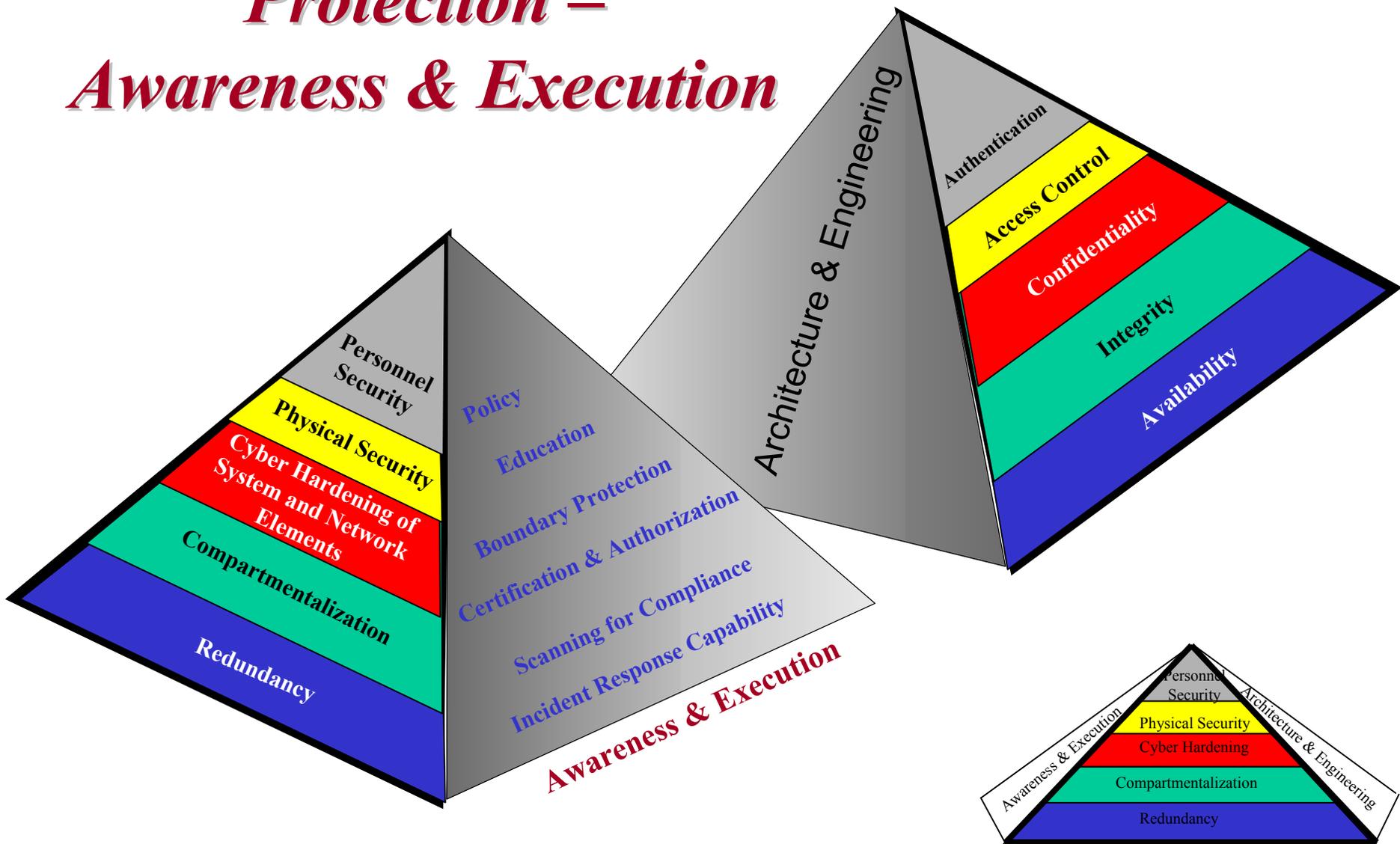
Code Red 24 hours

Slammer 30 minutes

Paradigm Shifts, Paradoxes, and Prognostications

- Harnessing the Infinite Resource
- Defending in the Face of Increasing Propagation Speeds
- Securing the Whole Even When Parts Have Been Compromised
- Prioritizing Amidst a Plethora of Alternatives
- Extending the Frontiers

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



Policy & Education

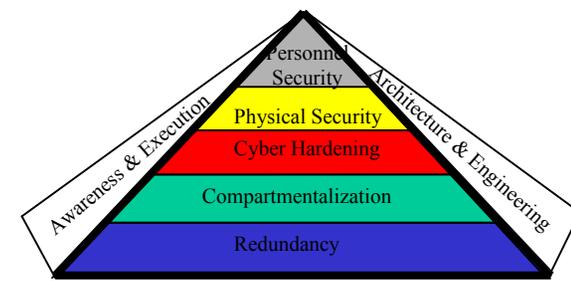
Policies are in place to address:

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.





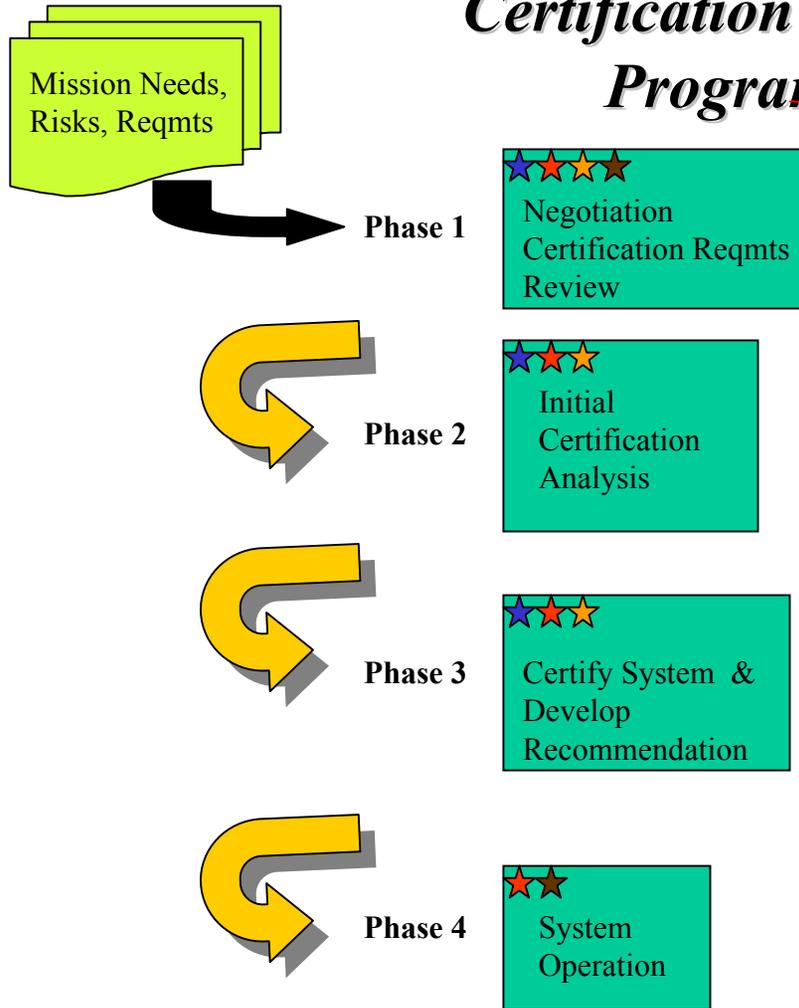
FAA's Cyber Defense Strategy

- 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

Securing Individual Systems

National Information Assurance Certification and Accreditation Program (NIACAP)

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

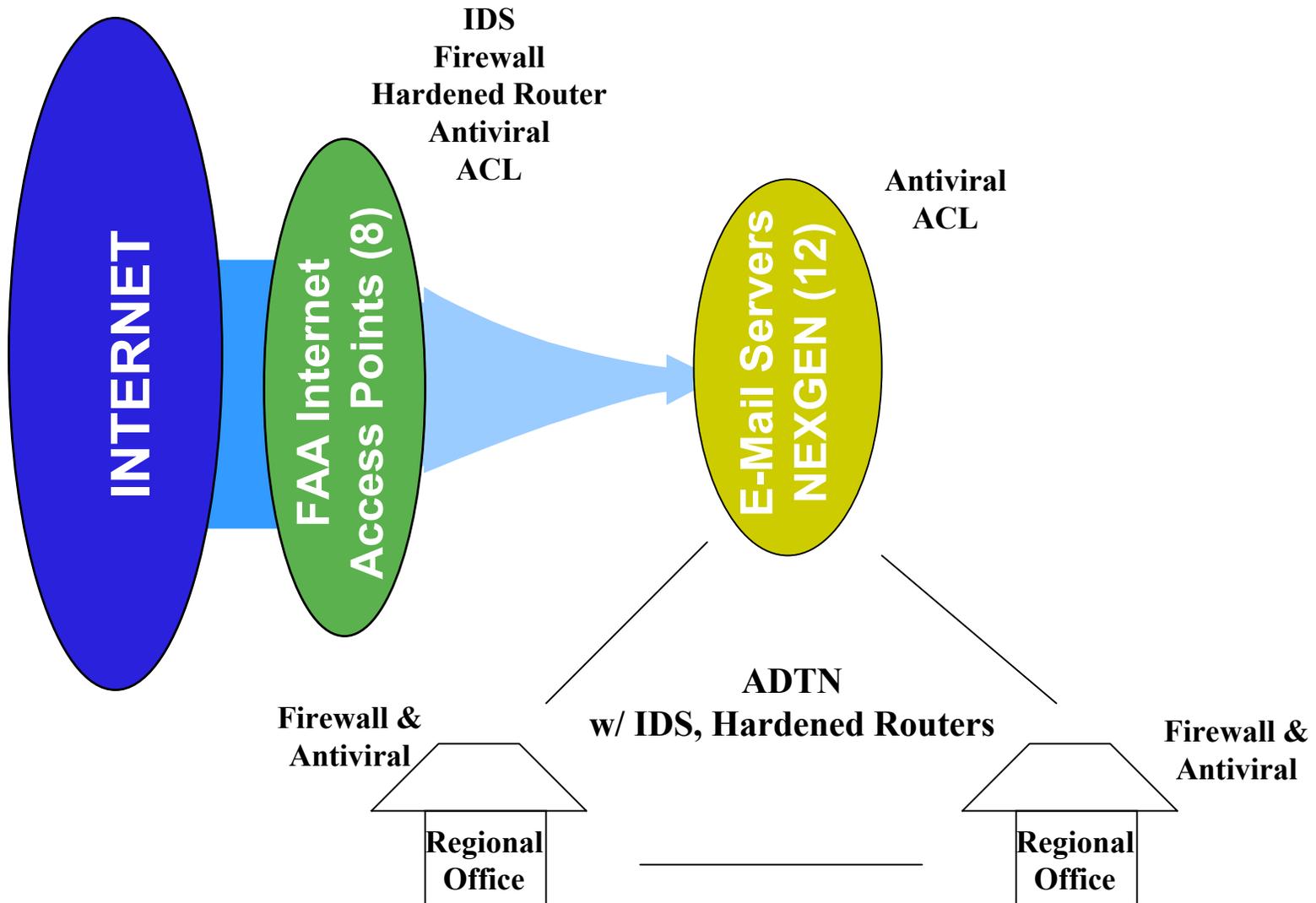


Nationally Recognized Process

**Security Requirements Review
During Milestone Zero**

Cradle to Grave Program

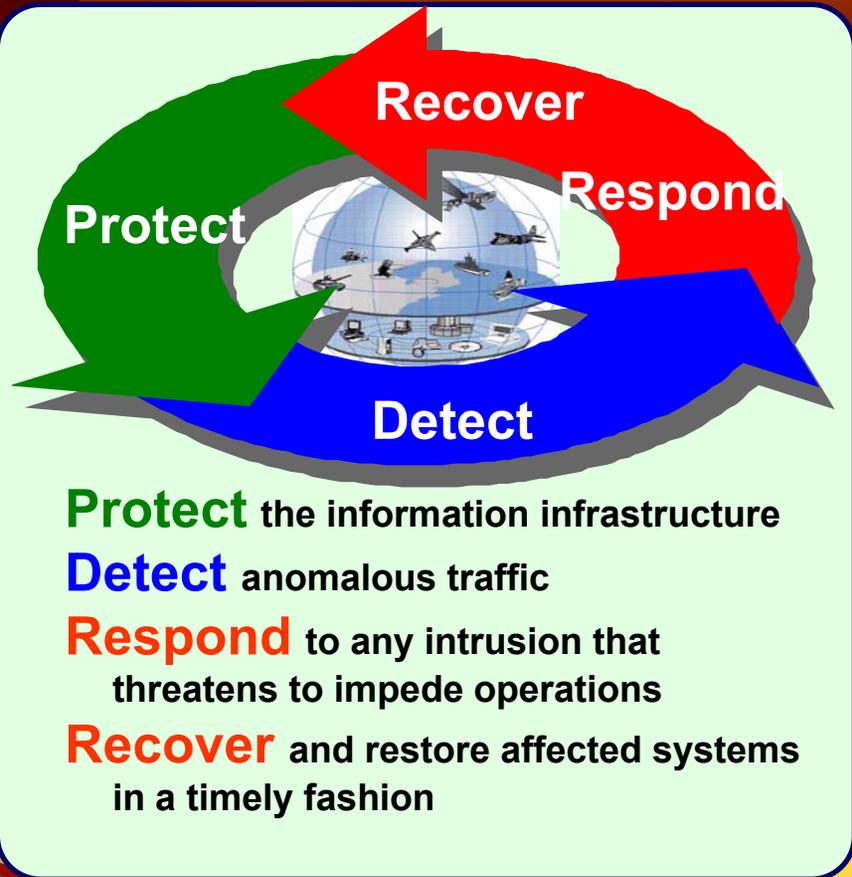
Boundary Protection



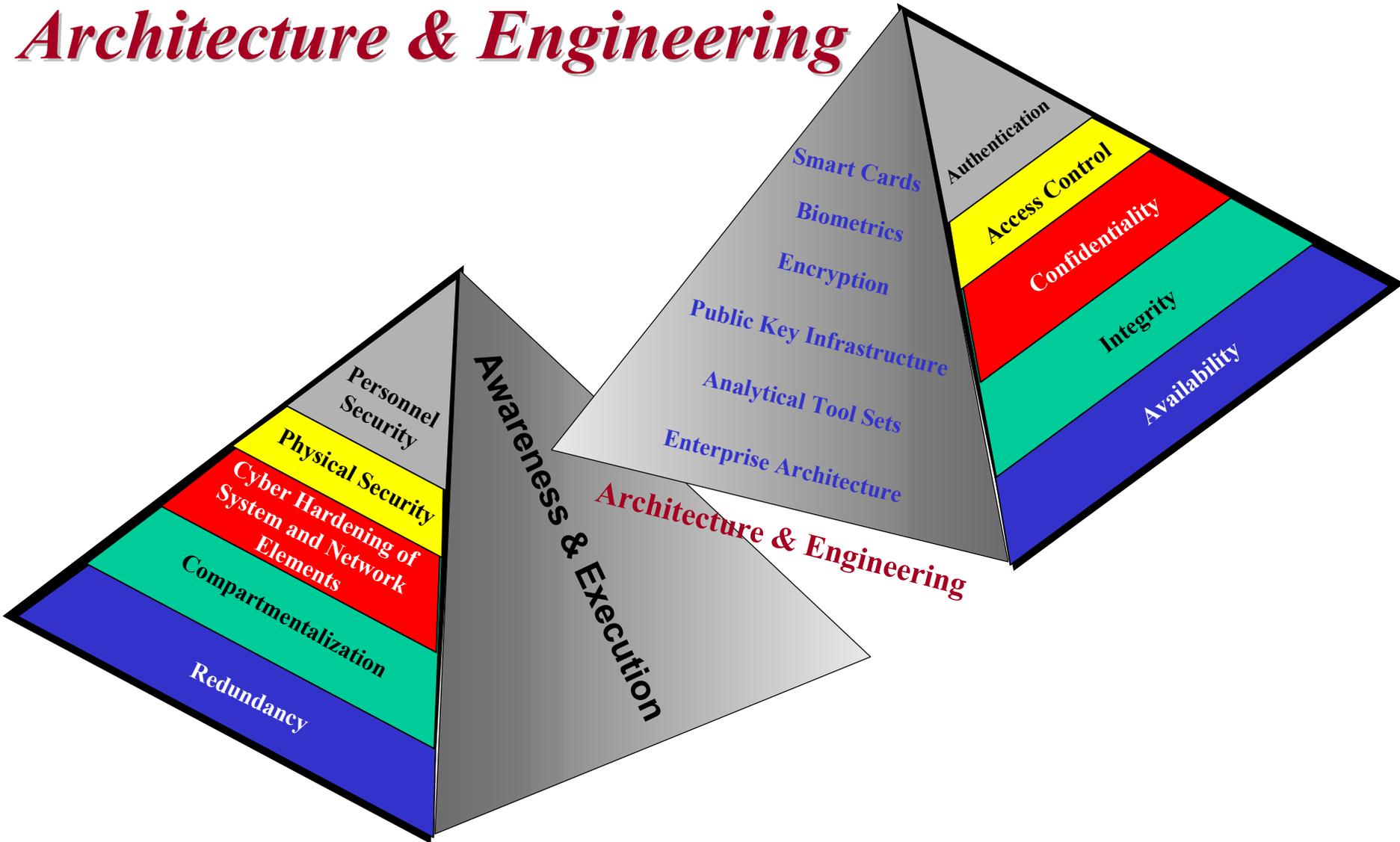
System Compliance Scanning Program

- 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

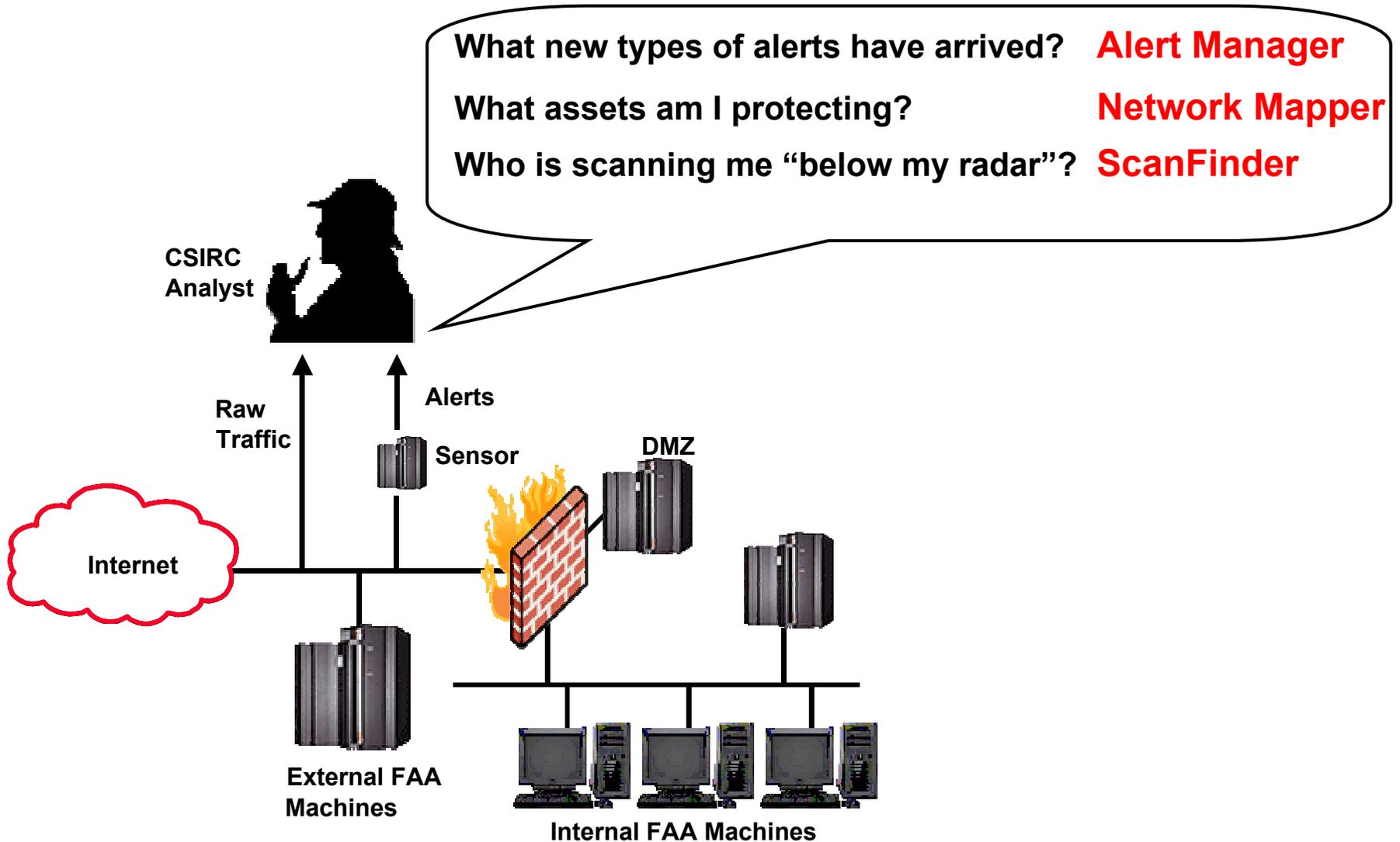
COMPUTER SECURITY INCIDENT RESPONSE CENTER (CSIRC)



FAA's 5 Layers of System Protection – Architecture & Engineering



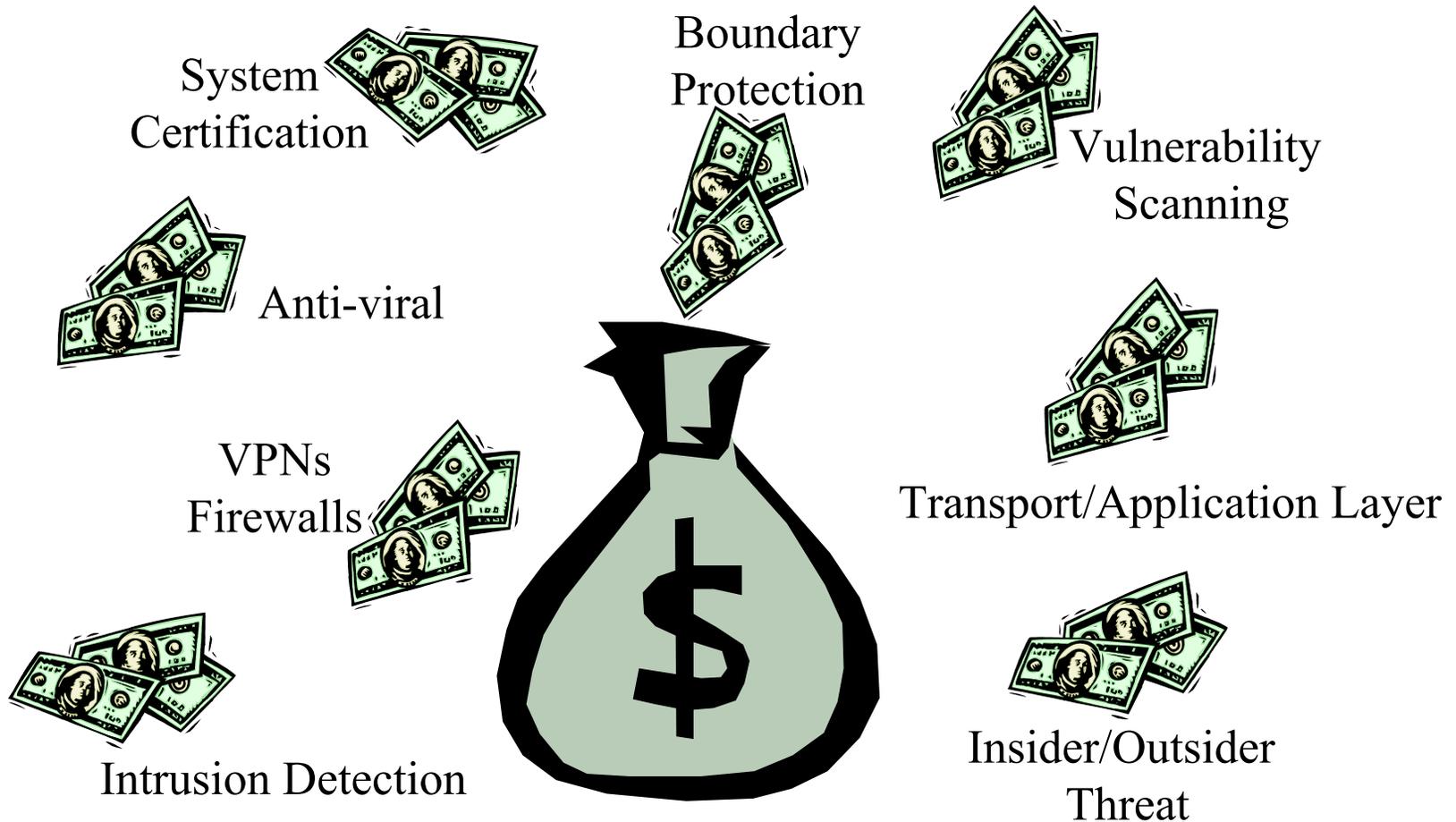
Mathematically-Based “Cool Tools”



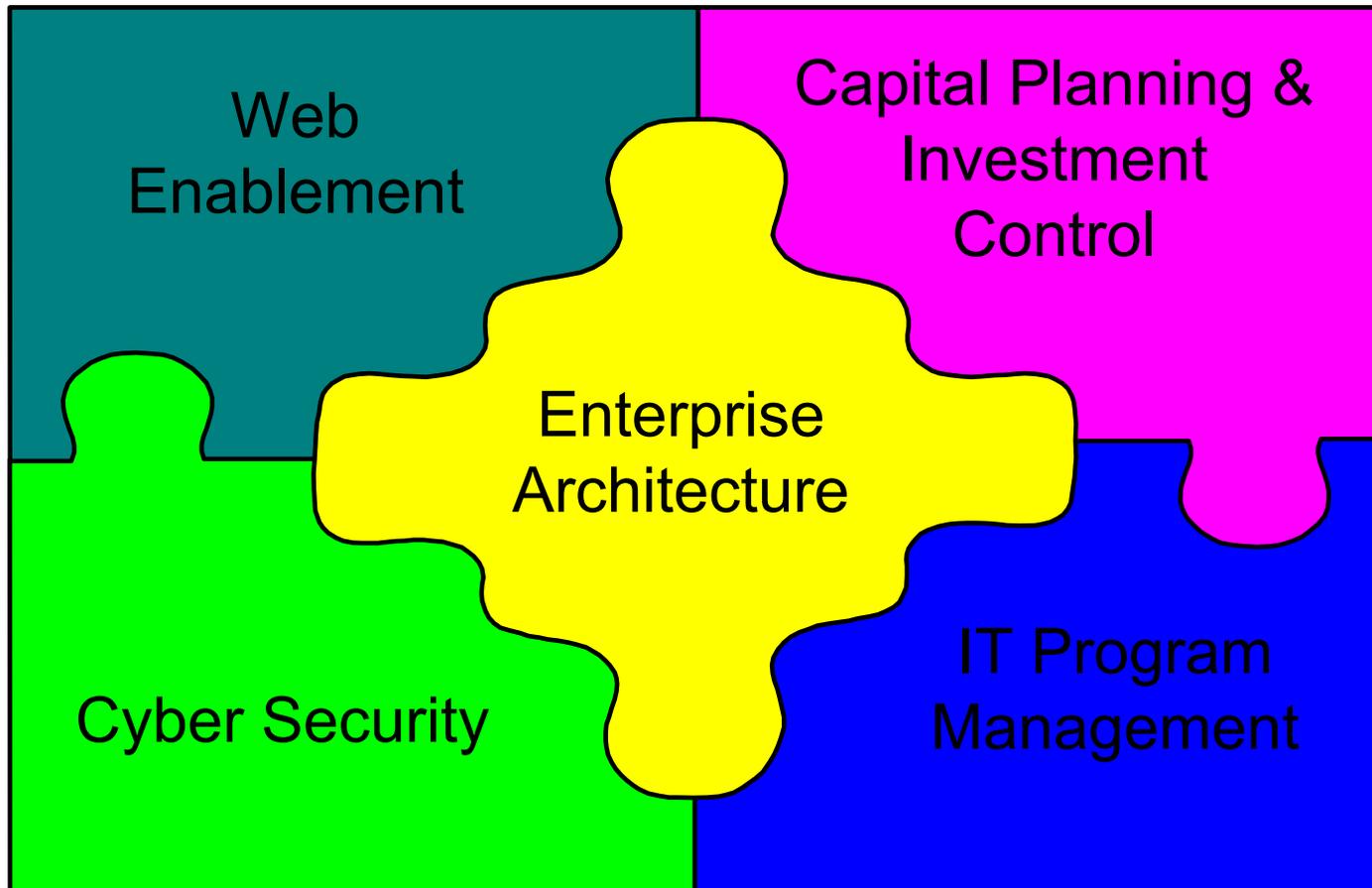
Paradigm Shifts, Paradoxes, and Prognostications

- Harnessing the Infinite Resource
- Defending in the Face of Increasing Propagation Speeds
- Securing the Whole Even When Parts Have Been Compromised
- Prioritizing Amidst a Plethora of Alternatives
- Extending the Frontiers

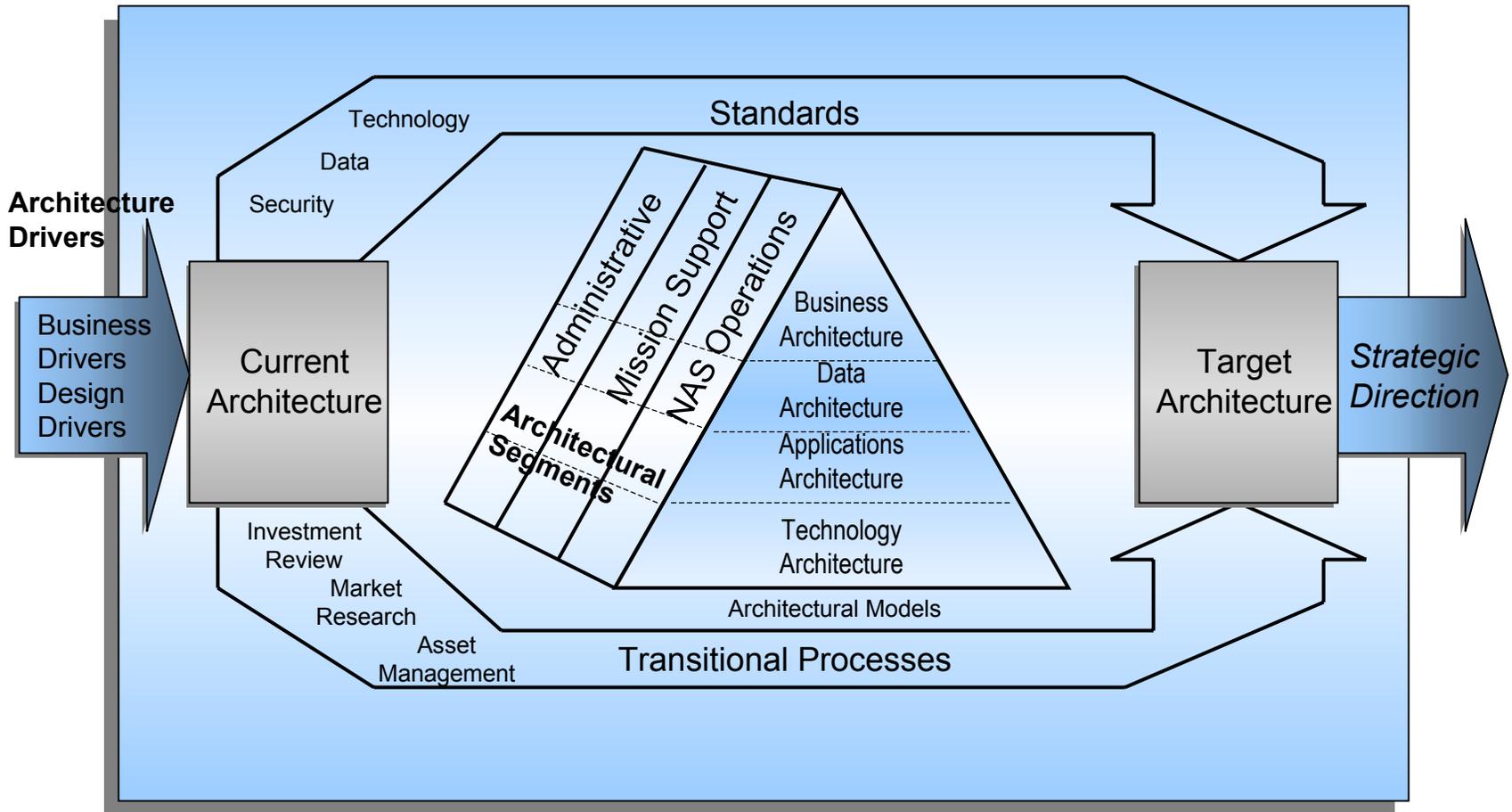
Money--The Scarce Resource



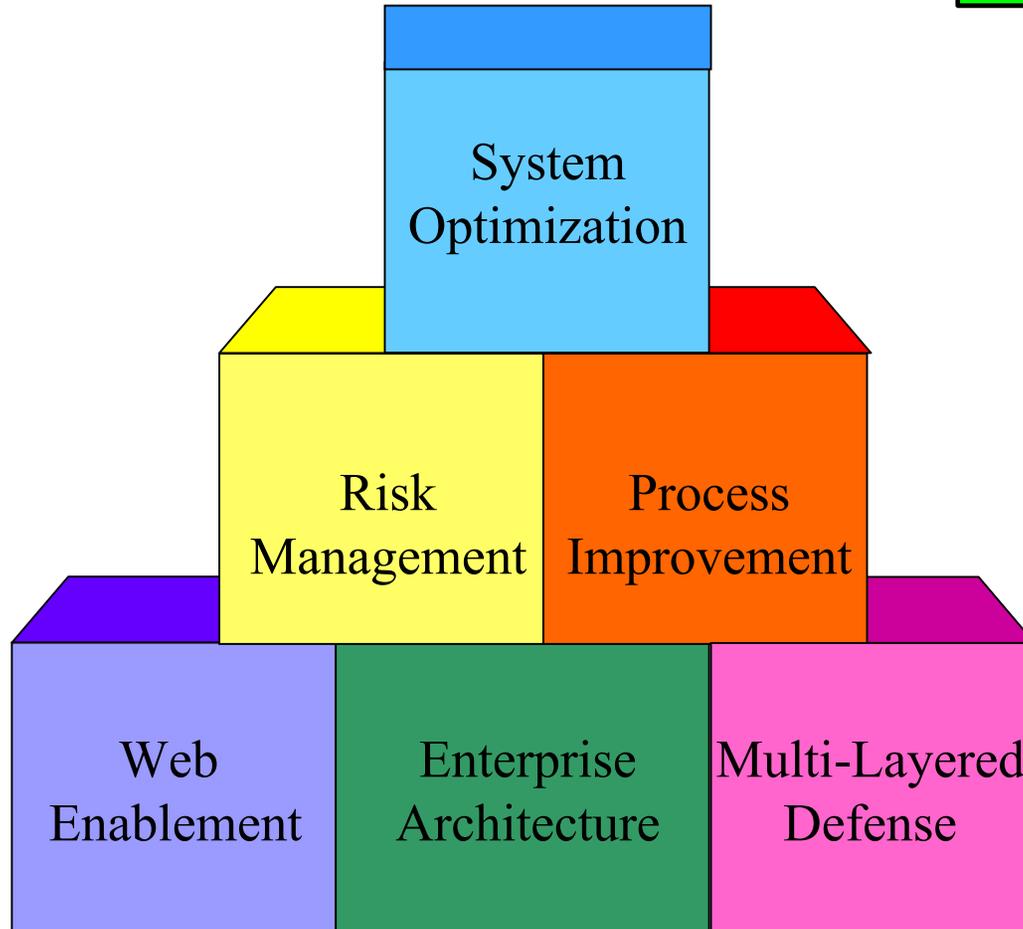
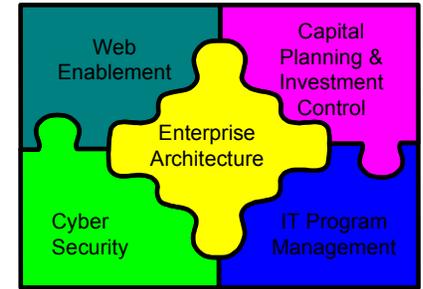
Enterprise Architecture as a Unifying Framework



Enterprise Architecture Framework



Enterprise Architecture as a Unifying Framework

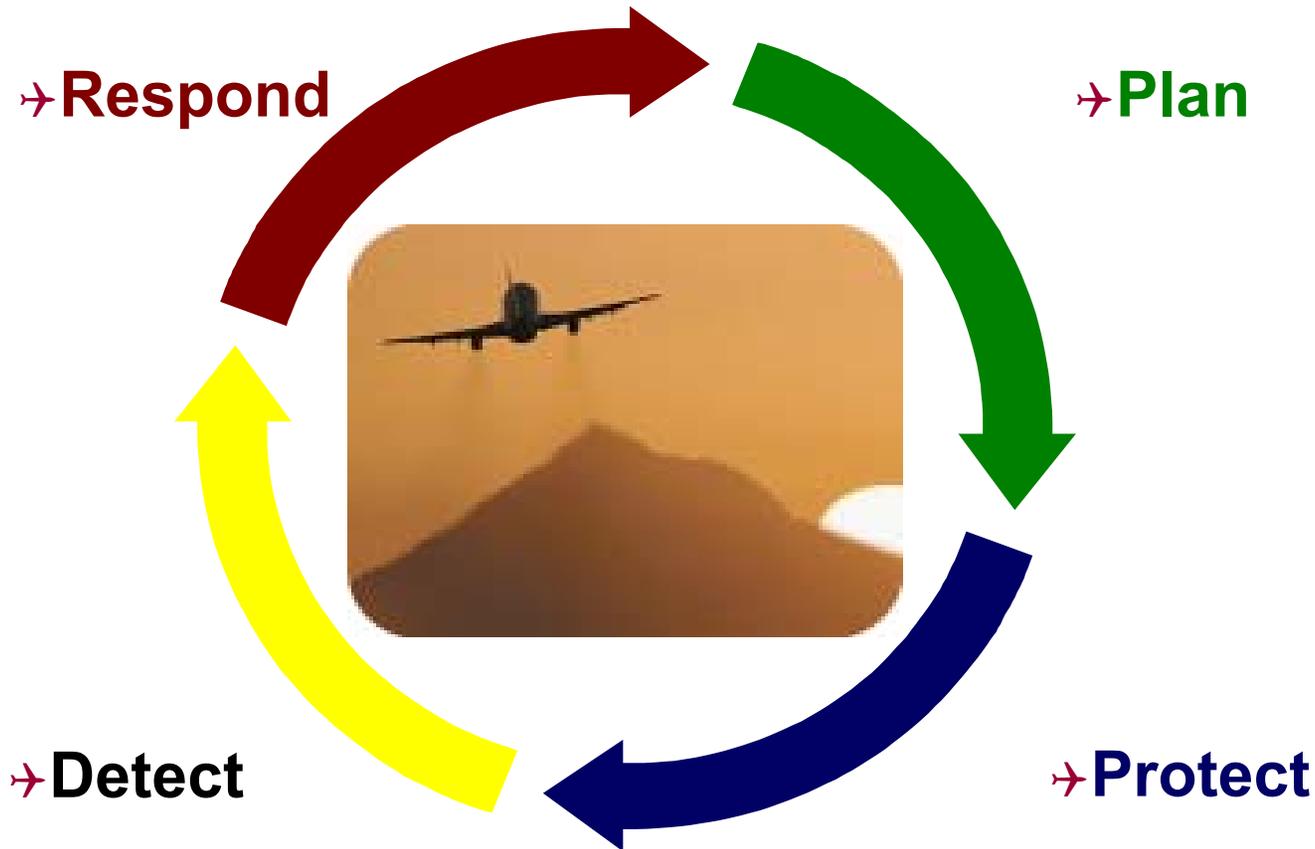


Paradigm Shifts, Paradoxes, and Prognostications

- Harnessing the Infinite Resource
- Defending in the Face of Increasing Propagation Speeds
- Securing the Whole Even When Parts Have Been Compromised
- Prioritizing Amidst a Plethora of Alternatives
- Extending the Frontiers

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





Extending the Frontiers

Private

Universities



Developers & Manufacturers

ISACs

010000100
0010000100
100010000100
0001000100001
0001000100001
0001000100001
0001000100001
0001000100001
0001000100001

Public



International

Professional Development

Continuous learning is an imperative

- Cyber Corps
- Computer Information Systems Security Professionals
- Specialized training with certifications for key personnel
- Awareness events for all FAA personnel
- Involvement in conferences and symposia on cyber security and enterprise architecture



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