Overview FAA IT & ISS R&D: Security Today Security Tomorrow

Marshall Potter
Chief Scientist for Information Technology
Federal Aviation Administration
AIO-4
(202) 267-9878
marshall.potter@faa.gov

Three FAA Mission Goals*

Safety: *Reduce fatal aviation accident rates by 80 percent in ten years*

Security: *Prevent security incidents in the aviation system*

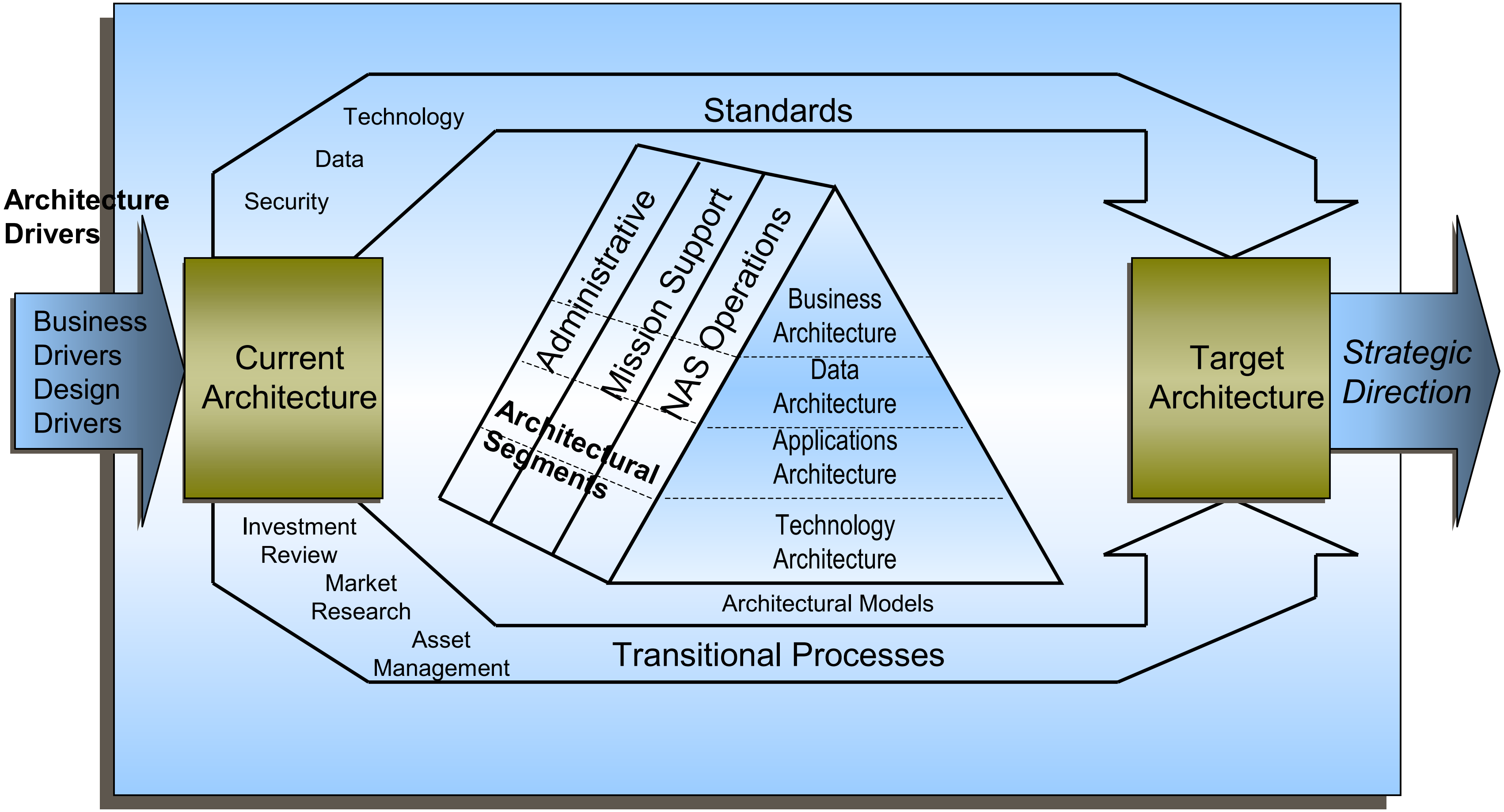
System Efficiency: *Provide an aerospace transportation system that meets the needs of users and is efficient in applying resources*

** FAA Strategic Plan*

Background: FAA...

- Is one of the largest civilian users of Information Technology
- Has growing demands for IT and system security
- Is responsible for security of a significant part of the Transportation Critical Infrastructure
- Must keep an eye to the future
- Must be aware of insider threats
- Needs Research and Development to meet its mission

Enterprise Architecture Framework Must understand the business architecture to secure the business



What is Information Security?*

- Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:
  - integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
  - confidentiality, which means preserving authorized restrictions on access an disclosure, including means for protecting personal privacy and proprietary information;
  - and availability, which means ensuring timely and reliable access to and use of information.

* FISMA

The CIO wants the ability to:

- Know how well our assets are protected
- Know the effort/cost of providing security
- Maintain our security
- Identify the “observables” of pending attacks
- Reduce the attack surface

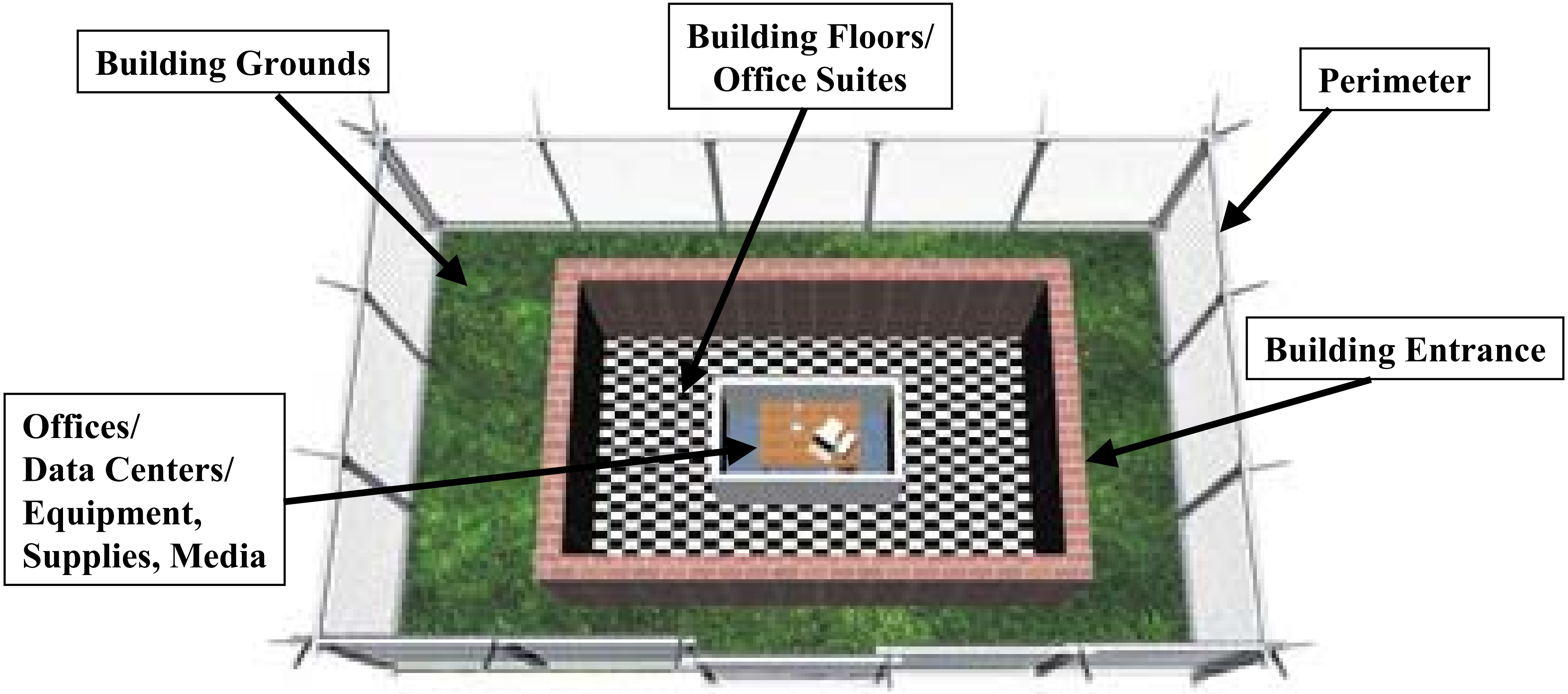
The CEO wants to know:

- How secure am I?
- Am I better off today than last year?
- Am I spending enough on security?
- What has my money accomplished?
- What's the value of my investment?
- What trends are we seeing?
- If I gave you $x, how would you invest it?

Security Today at the FAA

- Operational Security: Integrity and Availability
- Mission Support Security: Confidentiality
- Office of Information Services and Chief Information Officer
- Chief Scientist for Information Technology
- Office of Information Systems Security

Layered Defense Model



Building Grounds

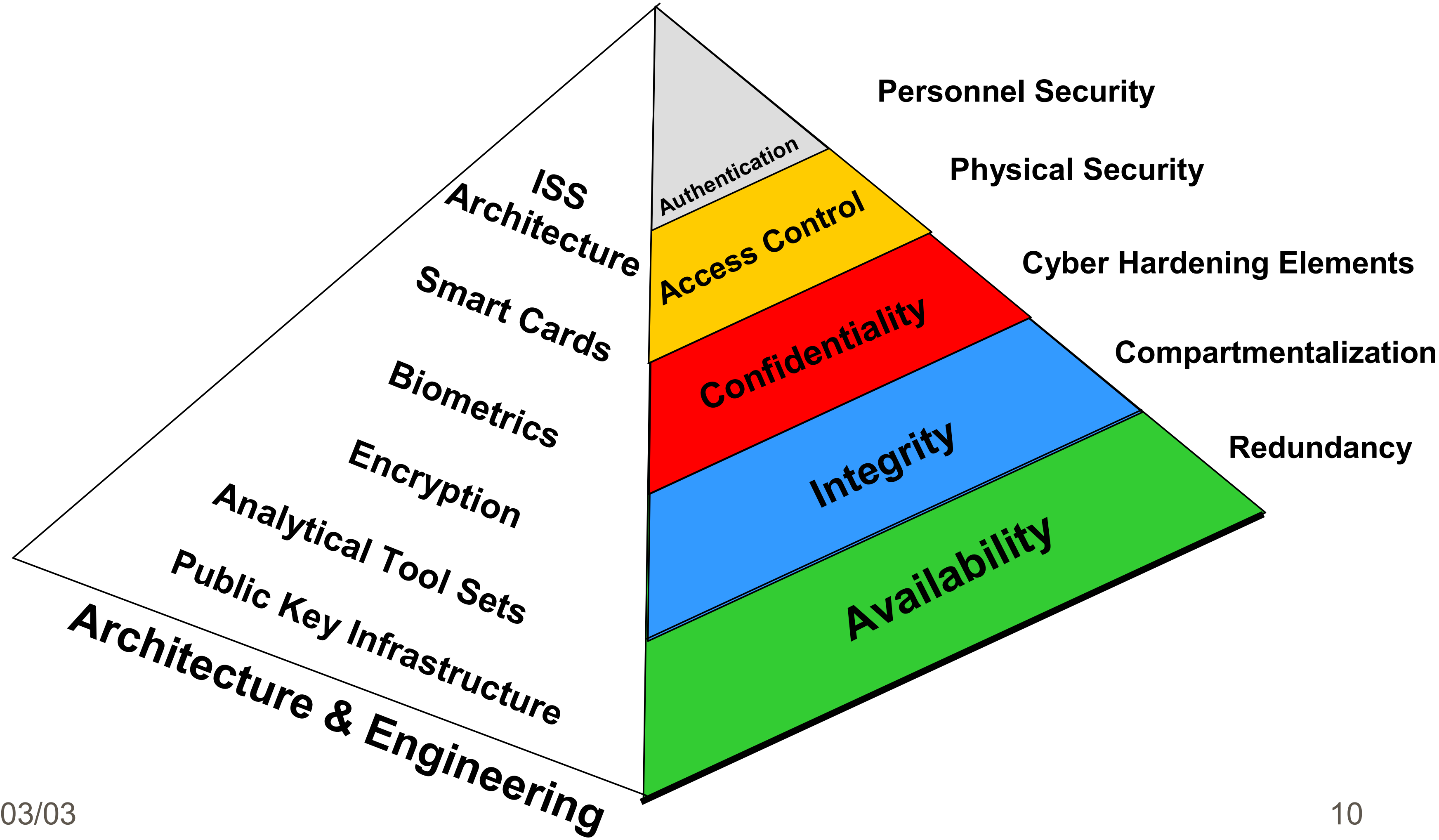
Building Floors/
Office Suites

Perimeter

Building Entrance

Offices/
Data Centers/
Equipment,
Supplies, Media

FAA's 5 Layers of System Protection



CSIRC

PREVENT

- Awareness and Training
- Patches and Fixes
- Vulnerability Testing

PROTECT

- Secure
- Provide Alerts, Advisories, Bulletins

DETECT

- Monitor
- Network with other CIRTS/CERTS

RESPOND

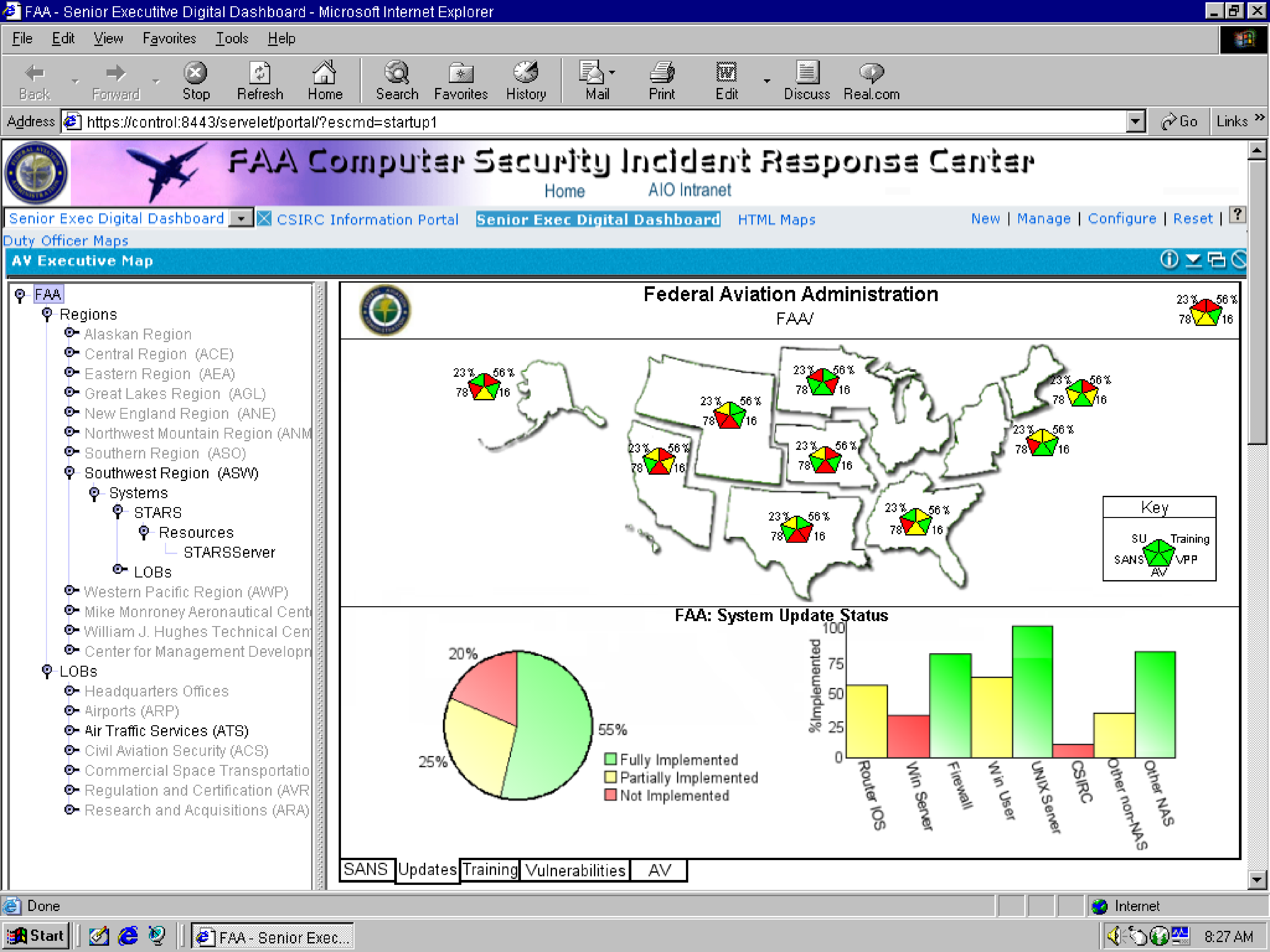
- Secure
- Prevent
- Block/Action

RECOVER

- Assist
- Provide Fixes

SECURITY BREACH:

1-866-580-1852


FAA - Senior Executive Digital Dashboard - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Edit
Discuss
Real.com
Address
https://control:8443/servelet/portal/?escmd=startup1
Go
Links
FAA Computer Security Incident Response Center
Home
AIO Intranet
Senior Exec Digital Dashboard
CSIRC Information Portal
Senior Exec Digital Dashboard
HTML Maps
New
Manage
Configure
Reset
?
Duty Officer Maps
AV Executive Map
FAA
Regions
Alaskan Region
Central Region (ACE)
Eastern Region (AEA)
Great Lakes Region (AGL)
New England Region (ANE)
Northwest Mountain Region (ANM
Southern Region (ASO)
Southwest Region (ASW)
Systems
STARS
Resources
STARSServer
LOBs
Western Pacific Region (AWP)
Mike Monroney Aeronautical Cent
William J. Hughes Technical Cen
Center for Management Developn
LOBs
Headquarters Offices
Airports (ARP)
Air Traffic Services (ATS)
Civil Aviation Security (ACS)
Commercial Space Transportatio
Regulation and Certification (AVR
Research and Acquisitions (ARA)
Federal Aviation Administration
FAA/
23 %
56 %
78
16
Key
SU
Training
SANS
VPP
AV
FAA: System Update Status
20%
55%
25%
Fully Implemented
Partially Implemented
Not Implemented
%Implemented
100
75
50
25
0
Router IOS
Win Server
Firewall
Win User
UNIX Server
CSIRC
Other non-NAS
Other NAS
SANS
Updates
Training
Vulnerabilities
AV
Done
Internet
Start
FAA - Senior Exec...
8:27 AM

Security Tomorrow: Three Thrusts of R&D

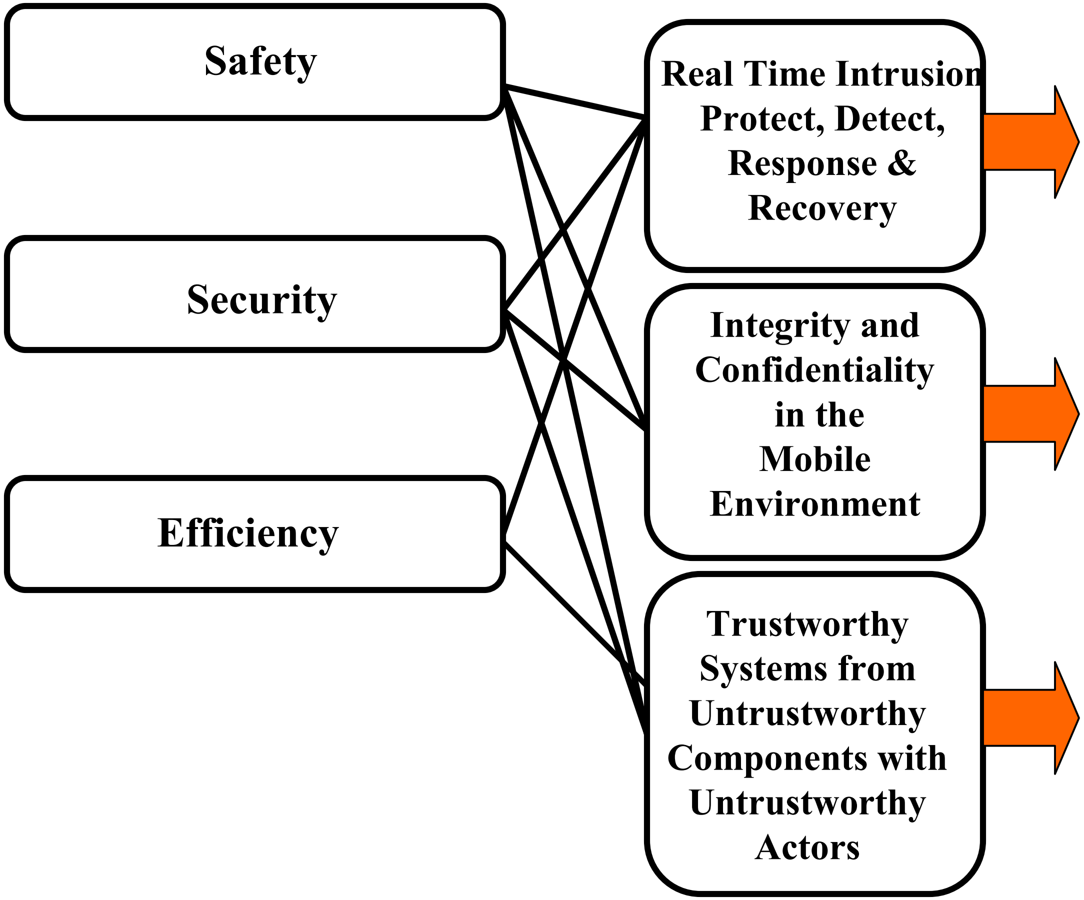
- **Real Time Intrusion Protect Detection, Response, & Recovery**
  - To provide continuity of operations in the face of attacks to FAA systems
- **Integrity and Confidentiality in the Mobile Environment**
  - Addresses the unique FAA mobile air-to-ground environment
- **Trustworthy Systems from Untrustworthy Components with Untrustworthy Actors**
  - The theory and impact of trust on security architectures

These overlap to cover safety, security, and efficiency

FAA R&D Initiatives

FAA Operational Goals

R&D
Focus Areas


Safety
Security
Efficiency
Real Time Intrusion Protect, Detect, Response & Recovery
Integrity and Confidentiality in the Mobile Environment
Trustworthy Systems from Untrustworthy Components with Untrustworthy Actors

Technology Needs

- Cyber Panel
- Incident classify & characterize
- Indicators and Warnings
- Intrusion Detect/Isolate
- Incident Response/Recovery
- ----------------
- Adaptive Survivable
  Infrastructure
- Cryptography (PKI, VPN)
- Identification & Authentication
- Malicious code protection
  Situational understanding
- Vulnerability Assessments
- ------------------
- Infrastructure: Adapt/Survive
- Boundary Protection
- Composable Trust
- Cryptography (PKI, VPN)
- Identification & Authentication
- Malicious code protection
  Situational understanding
  Models of Trust
- Vulnerability Assessments

Real Time Intrusion Protect Detection, Response, & Recovery

- **Protect – keep abreast of changing threats, and mitigate vulnerabilities**
- **Detection – CSIRC monitors networks, LAN and System Administrators keep close watch on internal and external traffic**
- **Response – Team in place responds appropriately to intrusions with minimal impact to operations**
- **Recovery – Effective contingency and disaster recovery plans to resume normal operations and inhibit repeat attacks**

Integrity and Availability in the Mobile Environment

- Collaborative R&D AFRL
  - Cyberwolf
  - DAIWatch
  - ATN IDS
- MIT Lincoln Labs/Natural Selection, Inc.

FAA In-House Tool Development for Improving Security Analyst Effectiveness

What assets am I protecting?	LanScape
Am I under widespread attack?	ATRaCT
Who is probing me “below my radar”?	Stethoscope
Which alerts are most important?	Alert Prioritizer

- Three prototype tools successfully deployed at the FAA CSIRC

  LanScape: Passively builds map of network assets (e.g., servers, services)

  ATRaCT: Detects alert trend changes

  Stethoscope: Detects slow, stealthy scans

- Ongoing R&D likely to result in FY04 Alert Prioritizer prototype tool
  - Detects successful (vs. attempted) attacks; dramatically reduces alert volumes
  - Detects anomalies to find novel attacks (exploits elliptical basis functions and evolutionary computation)

Integrity and Availability in the Mobile Environment

- **Integrity and Availability in an mobile environment addresses Air-Ground, wireless networks, LANs using diversity, public key infrastructure (PKI), and other technologies to reduce vulnerabilities**
- **Must concentrate on both RF and IR vulnerabilities**
- **Initial focus on CPDLC and airports**

Trustworthy Systems from Untrustworthy Components using Untrustworthy Actors

- Develop a (continuous/staged) model of trust
- Quarantine & Forensics
- Impacts on ISSA

Summary Slide

- There is no silver bullet
- Prioritization is the key to successful design
- Security must be dynamic and forward thinking
- We must maintain current vigilance while researching the world of tomorrow