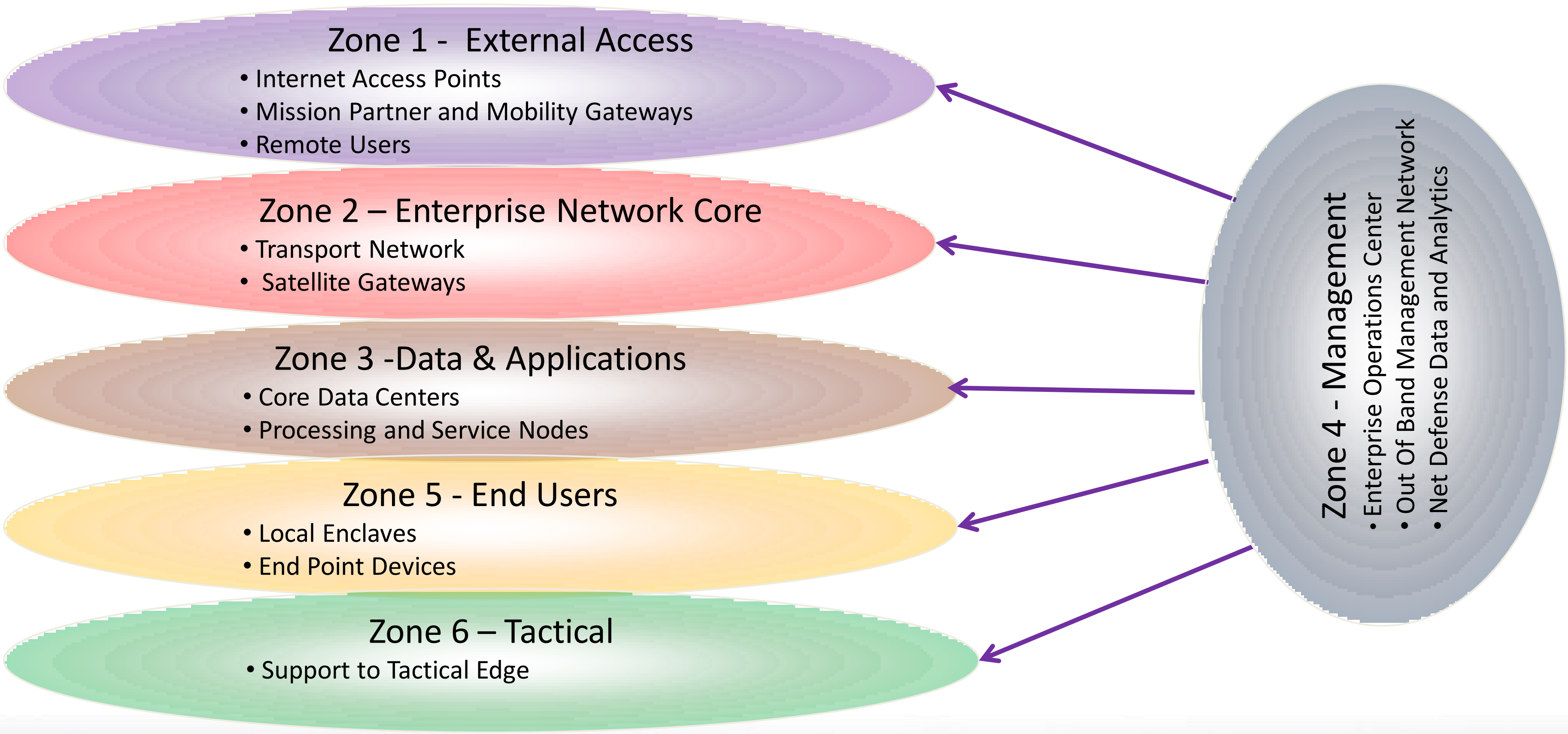
Cyber Defense

Mr. Bill Keely

Program Executive Officer – Mission Assurance

14 November 2013

JIE Security Architecture Zones



Zone 1 - External Access
- Internet Access Points
- Mission Partner and Mobility Gateways
- Remote Users

Zone 2 – Enterprise Network Core
- Transport Network
- Satellite Gateways

Zone 3 -Data & Applications
- Core Data Centers
- Processing and Service Nodes

Zone 5 - End Users
- Local Enclaves
- End Point Devices

Zone 6 – Tactical
- Support to Tactical Edge

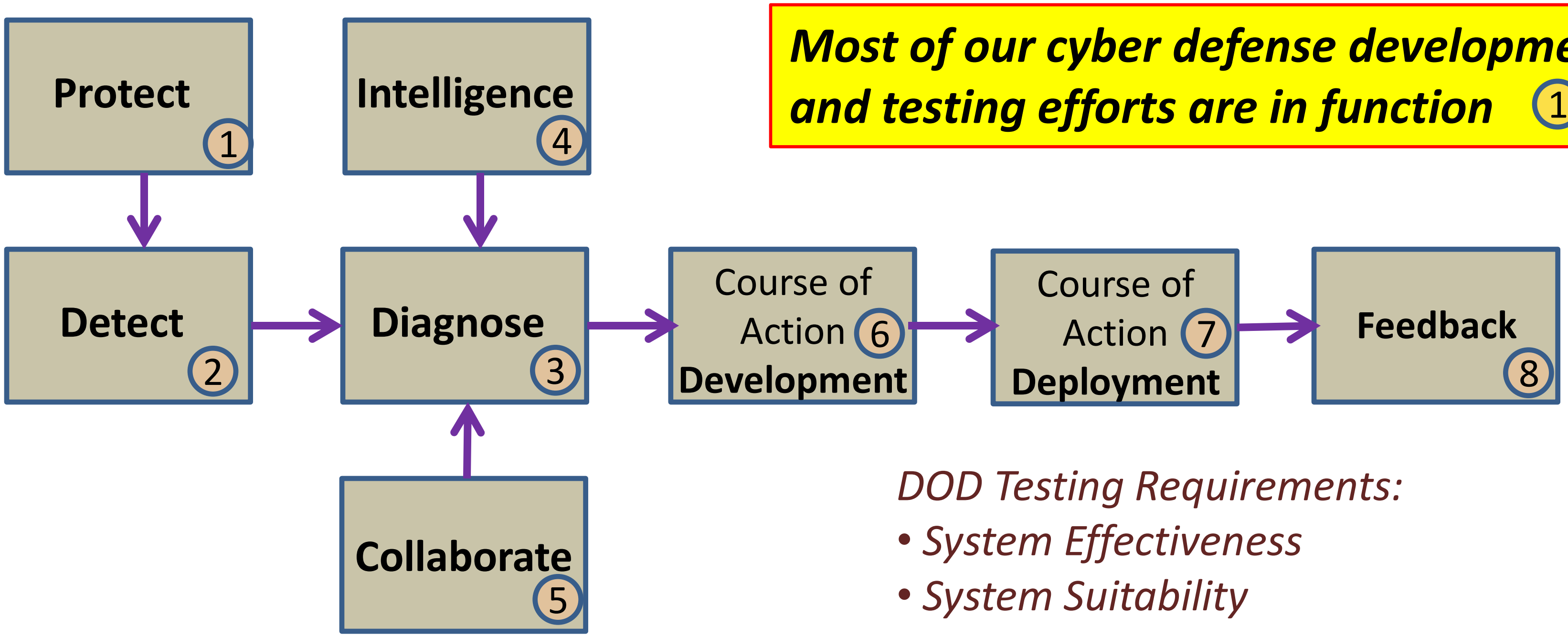
Zone 4 - Management
- Enterprise Operations Center
- Out Of Band Management Network
- Net Defense Data and Analytics

DISA
A Combat Support Agency

Enterprise Security Capabilities

- Zone 1 - External Access
  - Detect, block and counter targeted attacks at the Internet Access Points (IAP), including distributed denial of service and spear phishing (including: IDS/IPS, Enterprise Email Security Gateway)
  - Detect and block malicious and unauthorized web content (Web Content Filtering)
  - Controlled sharing of sensitive data (Mission Partner and Mobility Gateways, Cross Domain Solutions)
- Zone 2 – Enterprise Network Core
  - Block unauthorized and vulnerable ports and protocols
  - Detect and mitigate advanced persistent threats using backbone data collection sensors
  - Secure domain name servers
  - Secure satellite gateways
- Zone3 - Data and Applications
  - Protect and defend Core Data Centers and other processing and service nodes
  - Network data loss prevention
- Zone 4 – Management
  - Shared global situational awareness
  - Secure configuration management (technical security guidance, secure OS baselines)
  - Incident response (blue teams)
  - Secure out-of-band management
  - Readiness inspections and red teams
  - Cyber workforce training and education
- Zone 5 - End Users
  - Strong cyber identities for reduced anonymity (PKI, role based access control)
  - Real time detection and counter measures of host-based attacks (Host Based Security System (HBSS), anti-virus/anti-spyware)
  - Secure mobile devices
- Zone 6 -Tactical
  - Secure network operations at the tactical edge

Cyber Defense Functions



Protect 1

Intelligence 4

Detect 2

Diagnose 3

Course of Action 6 Development

Course of Action 7 Deployment

Feedback 8

Collaborate 5

Most of our cyber defense development and testing efforts are in function 1

DOD Testing Requirements:

- *System Effectiveness*
- *System Suitability*

1 Protect

- Passive Protections
- Architecture Design

2 Detect

- Network Sensors
- Host Sensors
- Logging

3 Diagnose

- False Positive Analysis
- Attack Characterization
- Counter Measures/Remediation

4 Intelligence

- Open Source
- Intell Updates

5 Collaborate

- Functional/Ops Community
- CNDSPs

6 COA Development

- Remediation Development
- Testing
- Deployment Synch/Planning

7 COA Deployment

- Packaging Change
- Distribution
- Support Desk

8 Feedback

- Effectiveness Analysis
- Residual Risk Analysis