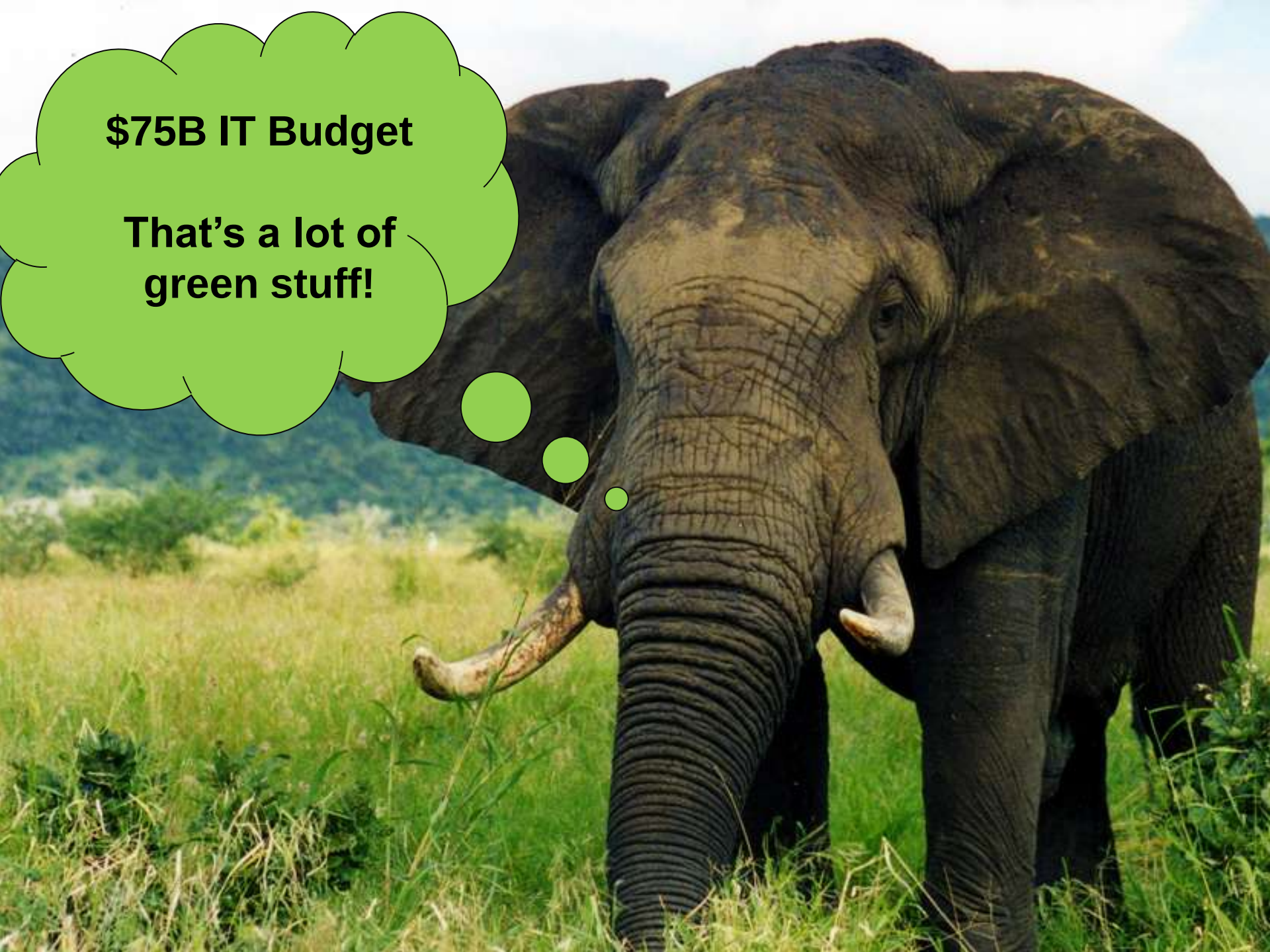
Massively Scaled Security Solutions for Massively Scaled IT

Michael Smith, SecTor 2009

Who is Michael Smith?

- 8 years active duty army
- Graduate of Russian basic course, Defense Language Institute, Monterey, CA
- DotCom survivor
- Infantryman, deployed to Afghanistan (2004)
- CISSP #50247 (2003), ISSEP (2005)
- Former CISO, Unisys Federal Service Delivery Center
- Currently a Manager in a Big Four Firm


$75B IT Budget
That’s a lot of green stuff!

Caveat!

Elephants don't turn on a dime, neither does the US Federal Government!

Federal Information Security Management Act

Roles & Responsibilities

- •Agency Head
- •CIO
- •Agency Security Officer

§3544(a)

Security Program

1. Periodic risk assessments
2. Policies and procedures
3. Security plans
4. Security awareness training
5. Periodic testing & evaluation
6. Remediation activities
7. Incident response capabilities
8. Continuity of operations

§3544(b)

Annual Security Review

- Determine sufficiency of security program
- Independent Evaluation (e.g., IG)
- Safeguard evaluation data

§§ 3544(c), 3545 (e)

Annual Reporting

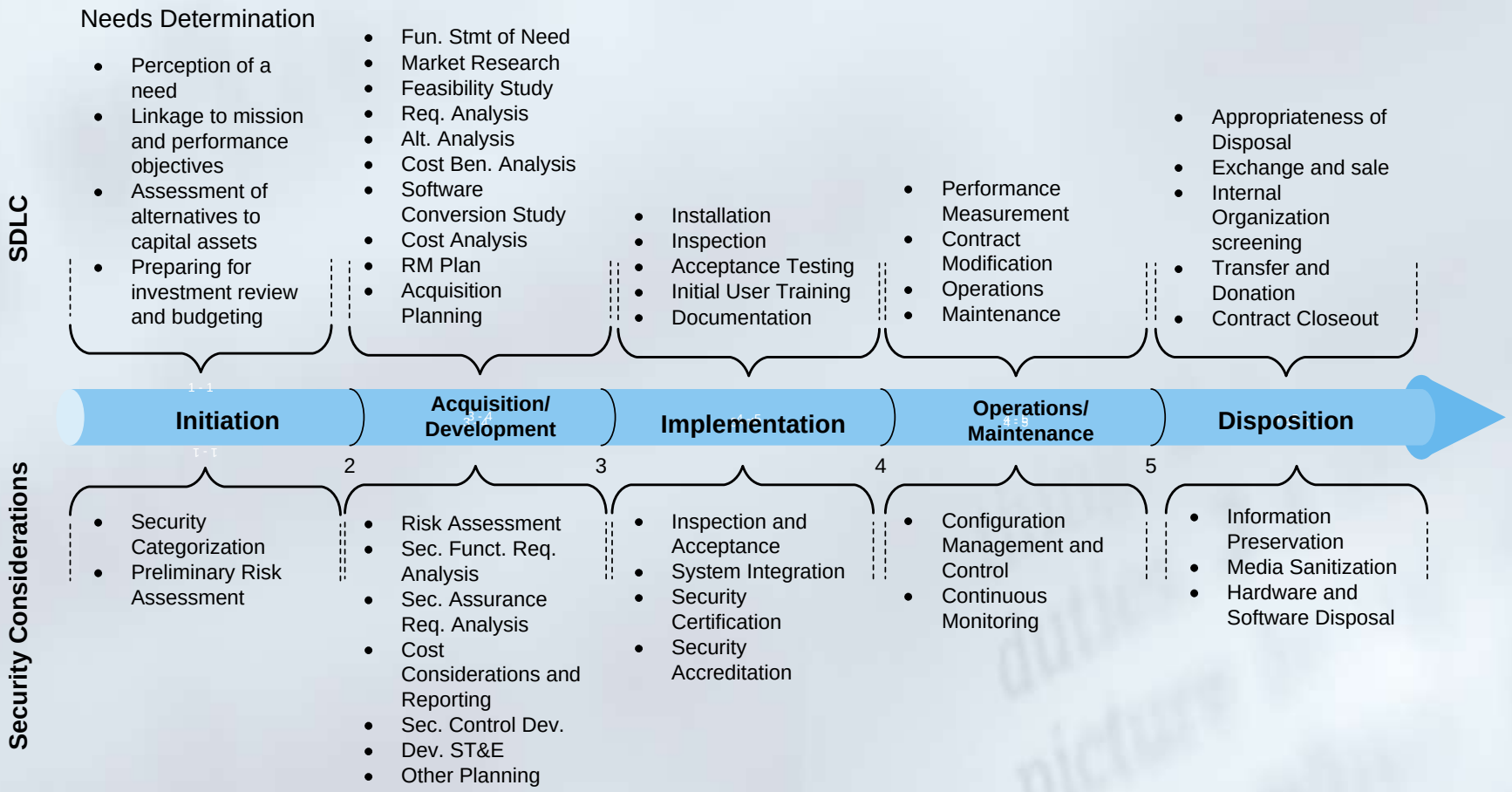
- •Reports from CIO & IG
- •Report material weaknesses
- •Provide performance plans

§§ 3544(c), 3545 (e)

The Standard Approach

- Break the elephant down into "bite-sized pieces"
- Group commonalities (common controls)
- Assess each piece—criticality, requirements, resulting risk
- Manage each piece individually
- Get better at securing each piece
- Caveat: each piece incurs overhead

Certification and Accreditation: IT Security in the SDLC



--NIST SP 800-64

HSPD-12

- "Standard" Smartcard for federal employees
- Cards used for 2-factor authentication
- Set of standards for PKI, issuance, clearances, etc

Think "Reduced sign-on and dual-factor identification federated throughout 50+ enterprises

Federal Desktop Core Configuration—FDCC

- Based on Air Force desktop configurations
- Attempts to be a Government-wide Security Technical Implementation Guide (STIG)
- Needs automated evaluation tools
- Part of the Federal Acquisition Regulation
- http://fdcc.nist.gov/

Security Control Automation Protocol—SCAP

- XML and protocols to exchange technical security information between products
- "Glue Code" between the following data sets:
  - Common Vulnerabilities and Exposures (CVE)
  - Common Configuration Enumeration (CCE)
  - Common Platform Enumeration (CPE)
  - Common Vulnerability Scoring System (CVSS)
  - Extensible Configuration Checklist Description Format (XCCDF)
  - Open Vulnerability and Assessment Language (OVAL)
- More products certified weekly

Trusted Internet Connections—TIC

- Reduce Government Internet connections to 50
- Lowers the demand for skilled personnel
- Uses models from DoD and DHS
- Agencies share Internet connections
- In theory: simplifies protecting Internet connections Government-wide
- http://www.whitehouse.gov/omb/memoranda/fy2008/m08-05.pdf

EINSTEIN

- Run by DHS and US-CERT
- National-Level Security Incident and Event Monitoring System
- Provides alerting and Government-wide threat trends
- Offered as a service to other agencies

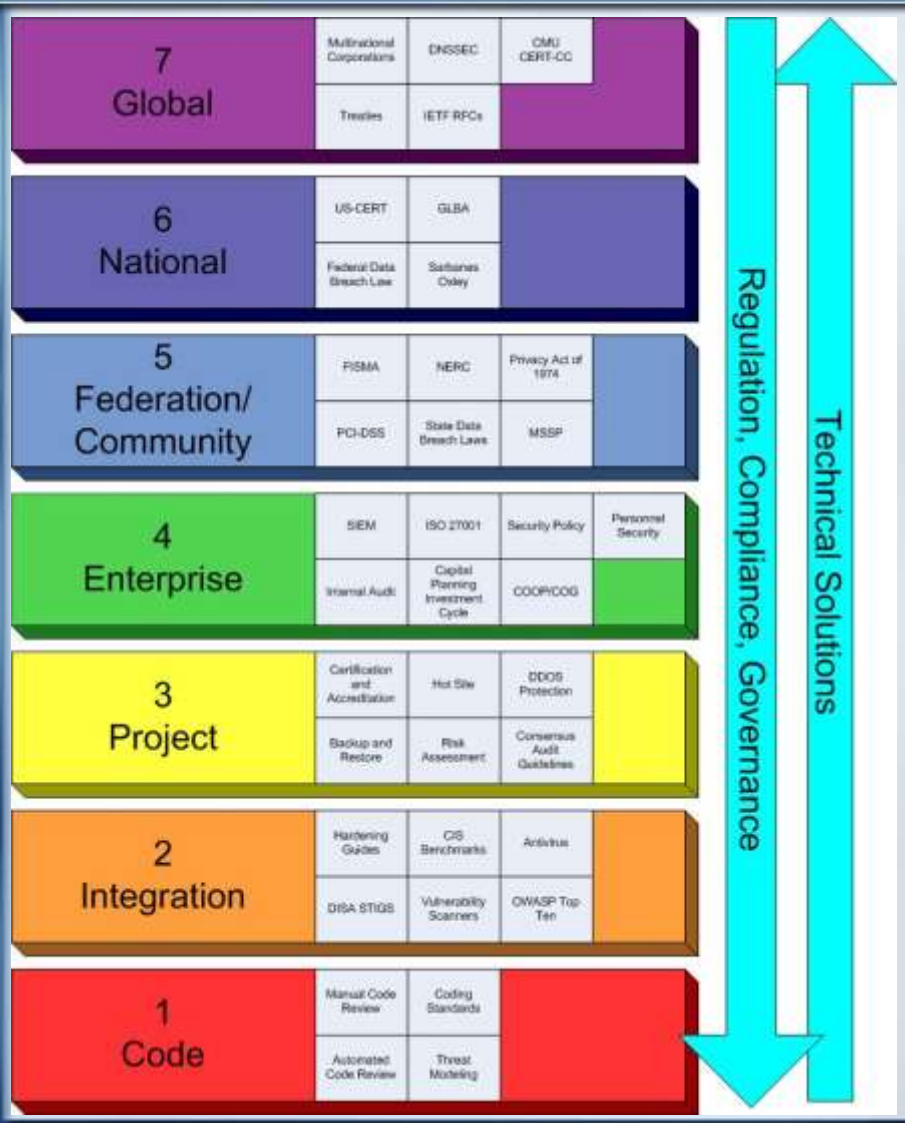
Standard Convergence

- One Government-wide standard for security management
- DCID 6/3 retired in favor of SP 800-37 and 800-53
- DoDI 8500.2 still in place but "bridged" to new convergent standards
- Transparent transition of people and process between civilian agencies, DoD components, and intelligence organizations

“Azimuth Check”

- Nobody knows where we’re going!
- Merging towards the center from regulation and technical solutions
- Enterprise gets the squeeze
- What about the pieces above the enterprise?
- We’re operating beyond the scope of traditional IT security doctrine, research, and products

My View of the World



- Each layer only knows the one above and below it
- Traditional IT security focuses on the Enterprise and Project layers

Existing Models of Management

History Lesson Time: thought you were just here to learn about security?


PERU
PHILIPPINES

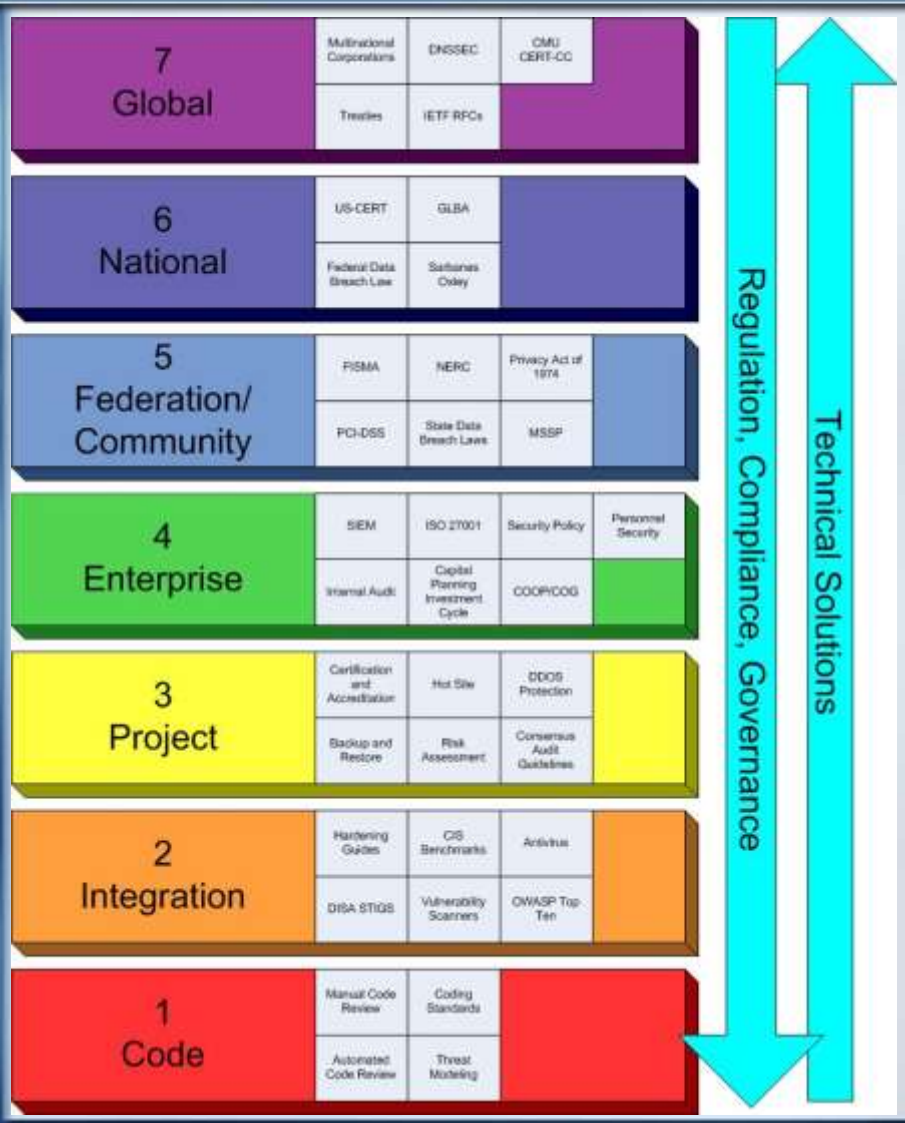

FUJITSU

Observations and Truthinesses

- Control v/s audit burdens
- Skill of the constituency
- Need a security professional at each layer

Is it all just a matter of centralized v/s decentralized?

The Models Begat More Questions…



- At what layer do you address a specific problem?
- Can a specific solution "scale up" to the Federation/ Community Layer?
- How do I get "clueful" people at each layer?
- How do I communicate between layers?

The Cybertastic Future: Management

- Use the Enterprise, Project, and Integration Layers
- Start in bite-sized pieces and consolidate wherever possible
- Need "clueful" people at all layers
- Organization at the Federation Layer for self-regulation—some people are already doing it

The Cybertastic Future: Process

- How do you keep from getting squeezed in the middle?
- If it's a pain for you, it probably is for others and can be scaled up
- How do we get information up to the higher layers so they can make a decision?

The Cybertastic Future: Vendors

- Support multiple 10-dot networks
- Products that tier between layers
- Federation and data import/export between products
- Compatibility with initiatives


Questions, Comments, or War Stories?
http://www.guerilla-ciso.com/
rybolov(a)ryzhe.ath.cx