

Security to the Edge: Towards Net-centric IA

March 6, 2007

Susan Alexander

Chief Technology Officer for Information and Network Assurance

Office of the Assistant Secretary of Defense, Networks and Information Integration/Chief Information Officer (OASD/NI) DOD/CIO

1

Governing Principles of Net-centric warfare



Governing Principles

- Fight first for *information superiority*
- Access to information: *shared awareness*
- *Speed of command* and decision making
- *Self-synchronization*
- *Dispersed forces*: non-contiguous operations
- *Demassification*
- *Deep sensor reach*
- *Alter initial conditions* at higher rates of change
- *Compressed operations* and levels of war

2

GIG Buzz-phrases



- Power to the edge (decentralized Command and Control)
 - Net-centric enterprise services (NCES)
 - Policy-based authorization (ABAC, RADAC)
- Post before process with infinite reachback
 - DOD Data strategy
 - TPPU vs TPED
- Net-readiness (KPP)
- Dynamic communities of interest (COIs)
- Horizontal Fusion

3

So what's so different?



- Massively **distributed** enterprise of (mostly) non-replicated resources – *integrity, availability*
- Blurring of tactical and strategic, with **every node a portal into the whole**
- Notion that access will be based upon **user's need** rather than originator's permission – *balancing confidentiality with availability*
- **Net-centric provisioning** (including C2) for agility and flexibility
- Reliance upon **remote** and **anonymous** nodes - *authenticity, integrity*

*In a Nutshell:
the need for "Distributed Trust"*

4

GIG as a combat system IA imperatives



Aiming the gun: Information advantage for superior decision making

- Maximum accessibility of data for mission while denying knowledge to adversaries
- Seamless collaboration with mission partners

Shoots where I point: Trustworthy and robust platform for executing intent

- Command and control never subverted
- Service is available

Works under fire

- Attacks are prevented or deflected
- Can recover from *successful* attacks
- Operate through

5

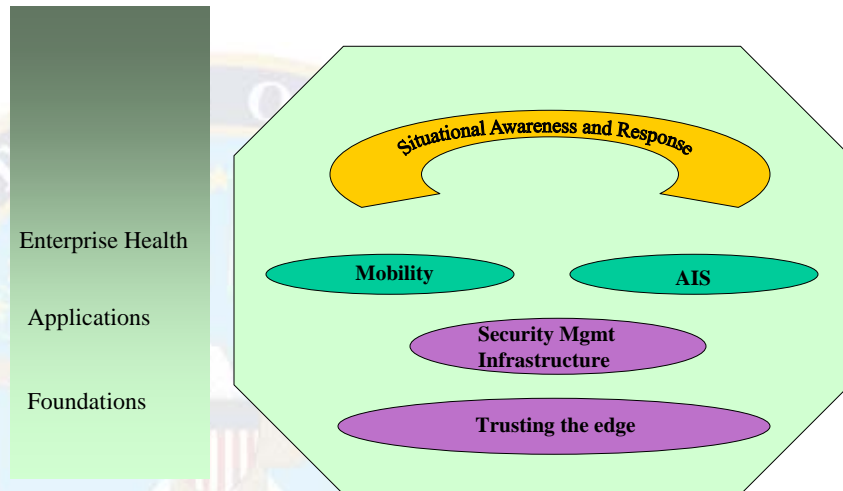
Back-up Slides



Some of the technology under the hood

6

Security to the Edge Construct



7

Security management infrastructure



- Attribute management
 - Identity, location, role, trustworthiness
 - Sensing, authenticating
 - Humans, non-humans
- Privilege management
 - Resource access, command and control
- Policy management
 - Global rules of engagement, local policy
 - Dynamic risk calculation

8

Trusting the edge



- Self-protecting in a hostile environment
 - Hardware
 - Software
- Remotely interrogable integrity
 - Measurement
 - Attestation

9

Assured Information Sharing



- Must support arbitrary policy and object granularity
- Converges to one network
- Supports augmentation with *guest* infrastructures
- Guarantees integrity of information

10

Mobility



- Worldwide access anytime, anywhere
- One piece of gear
- Location-specific behavior
- Must not be overheard
- Must not become a **glowing** target

11

Enterprise Health



- *Availability* is key to NCW
- Though often overlooked, so is *integrity*
- Adversary response vs. hygiene factors
- Might pay to integrate with SMI
- Huge problem– Good news is, everyone is working on it!

12