Securing Content in the Department of Defense's Global Information Grid

Secure Knowledge Management Workshop
State University of New York - Buffalo

23-24 September 2004

Robert W. McGraw
Technical Director
IA Architecture & Systems Security Engineering Group
Information Assurance Directorate
National Security Agency

Vision for DoD Transformation

The Department of Defense is transforming itself through the Global Information Grid (GIG) in pursuit of information superiority and net-centric warfare (NCW)

"The two truly transforming things might be in information technology and information operating and networking… connecting things in ways that they function totally differently than they had previously."

"And if that's possible…then possibly the single most transforming thing in our Force will not be a weapon system, but a set of interconnections and a substantially enhanced capability because of that awareness."

Donald Rumsfeld, Secretary of Defense
Town Hall Meeting, Pentagon, 9 August 2001

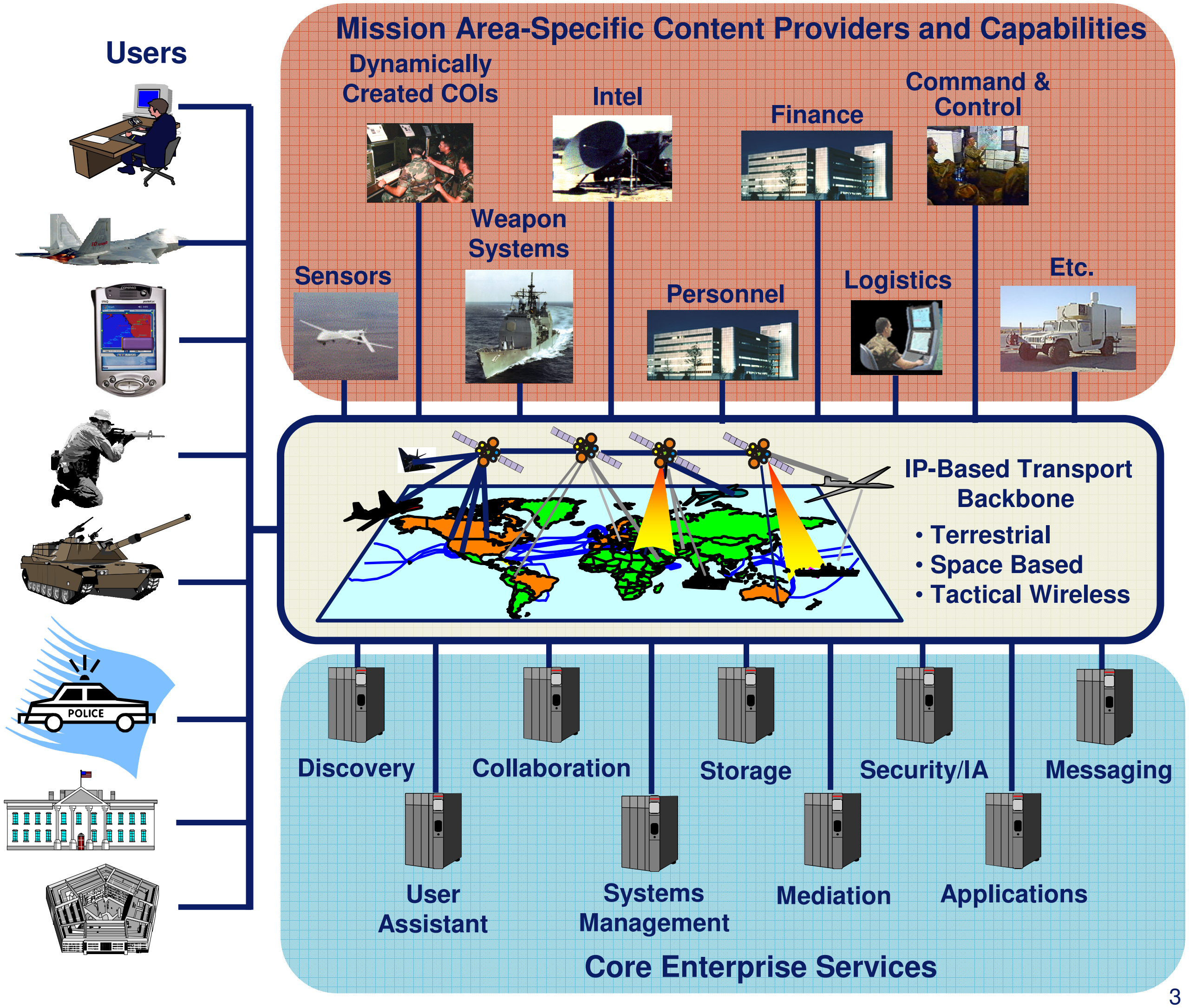
"…the outcome we must achieve: fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battlefield"

Donald Rumsfeld, Secretary of Defense
Secretary's Foreword to Transformation Planning Guidance, April 2003

GIG Vision

Fundamental transformation in information/content management, communications, and information assurance.

- **IP Transport Backbone**
  - Fiber
  - Satellite
  - Wireless
  - Highly Available
- **Service Oriented Architecture**
  - Core Enterprise Services
  - Unique Mission Specific services
- **Content Providers**
  - Provided by mission specific entities
  - Many mission areas (e.g. business, financial, personnel, command and control, intelligence, warfighting)
- **Users**
  - Consumers of the GIG content. DoD Intelligence Community, Allies and coalition partners, other government, state/local…



Users

Mission Area-Specific Content Providers and Capabilities

Dynamically Created COIs

Intel

Finance

Command & Control

Weapon Systems

Sensors

Personnel

Logistics

Etc.

IP-Based Transport Backbone

- Terrestrial
- Space Based
- Tactical Wireless

Discovery

Collaboration

Storage

Security/IA

Messaging

User Assistant

Systems Management

Mediation

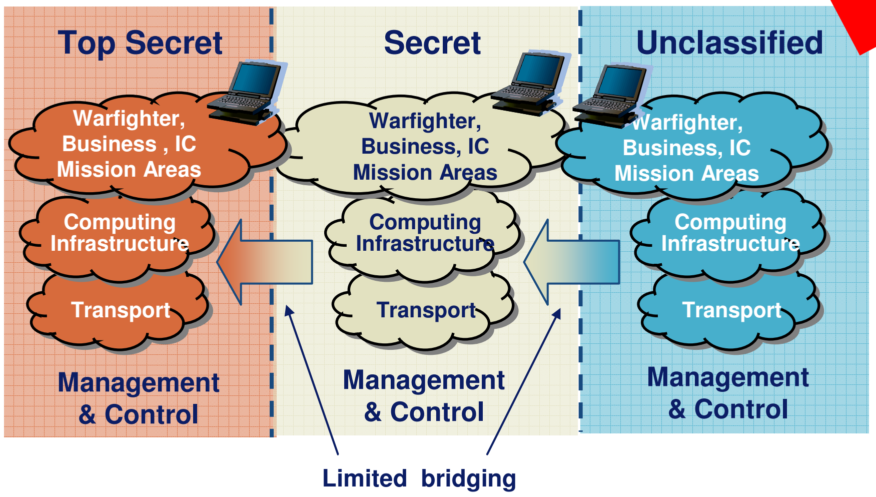
Applications

Core Enterprise Services

GIG Transformation Drives Focus on IA and Securing Content

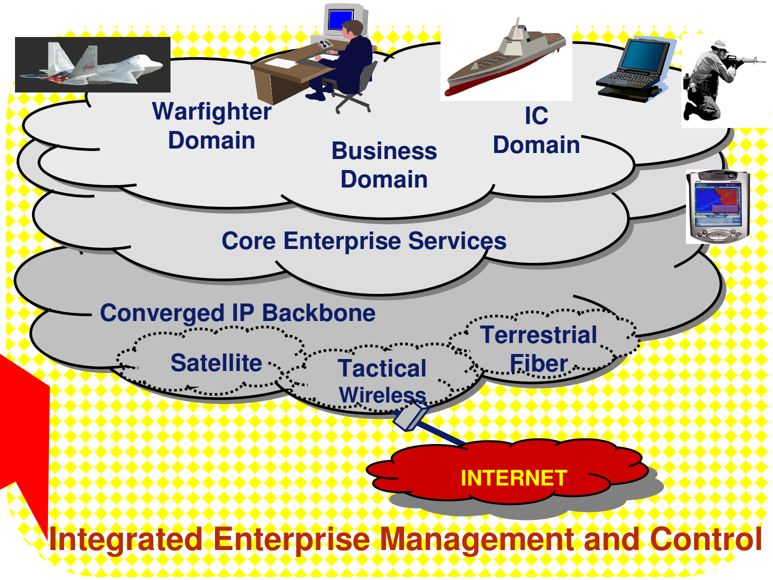
Current (Conceptual)

- Separate networks that rely on physical, cryptographic, and administrative isolation to protect content of different sensitivity
- Isolation approach restricts ability to share content by creating stovepipes with limited bridging



Incremental Evolution

Future (implied by GIG vision)

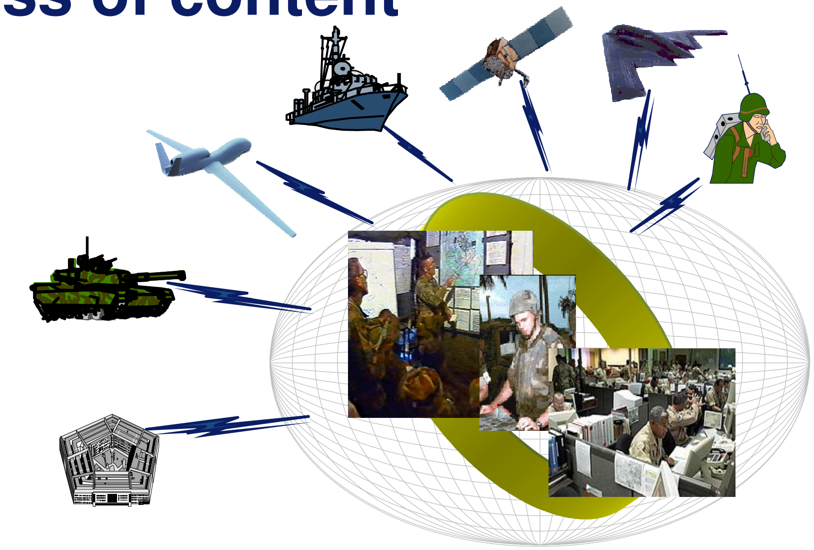


- Common, converged networks that rely on advanced Information Assurance technologies and trustworthy systems to protect content of different sensitivity
- Ubiquitous Information Assurance enables content sharing through logical domains and communities of interest

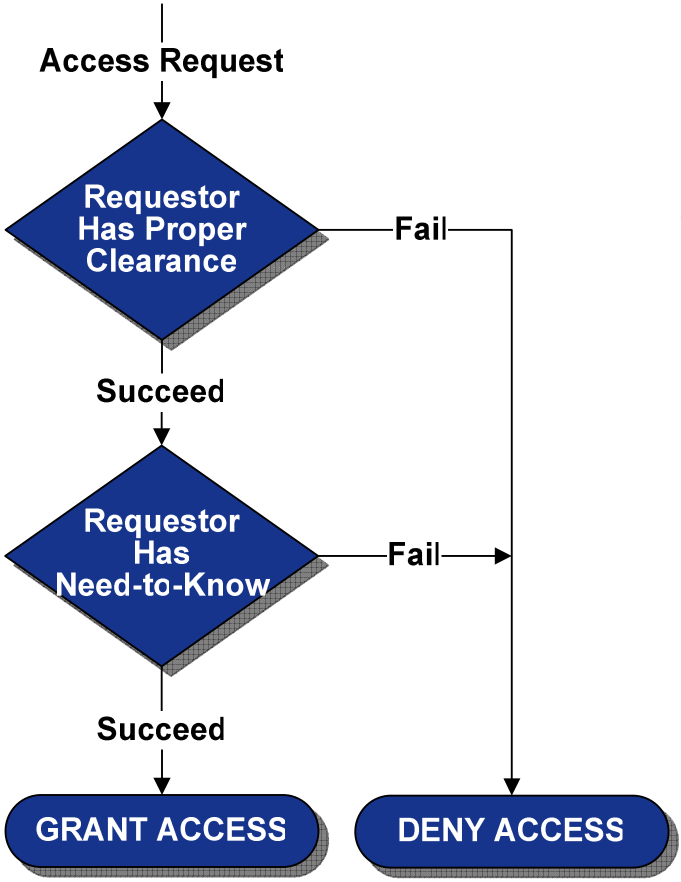
Some Considerations for Securing Content in the GIG

Goal: Ensure that the content relied upon by GIG users is properly protected, available, reliable, and authorized for use, in a common, coordinated manner.

- Security Risk Assessment
- Content types
- Reliability and trustworthiness of content
- Availability of content
- Robustness of systems
- Access control



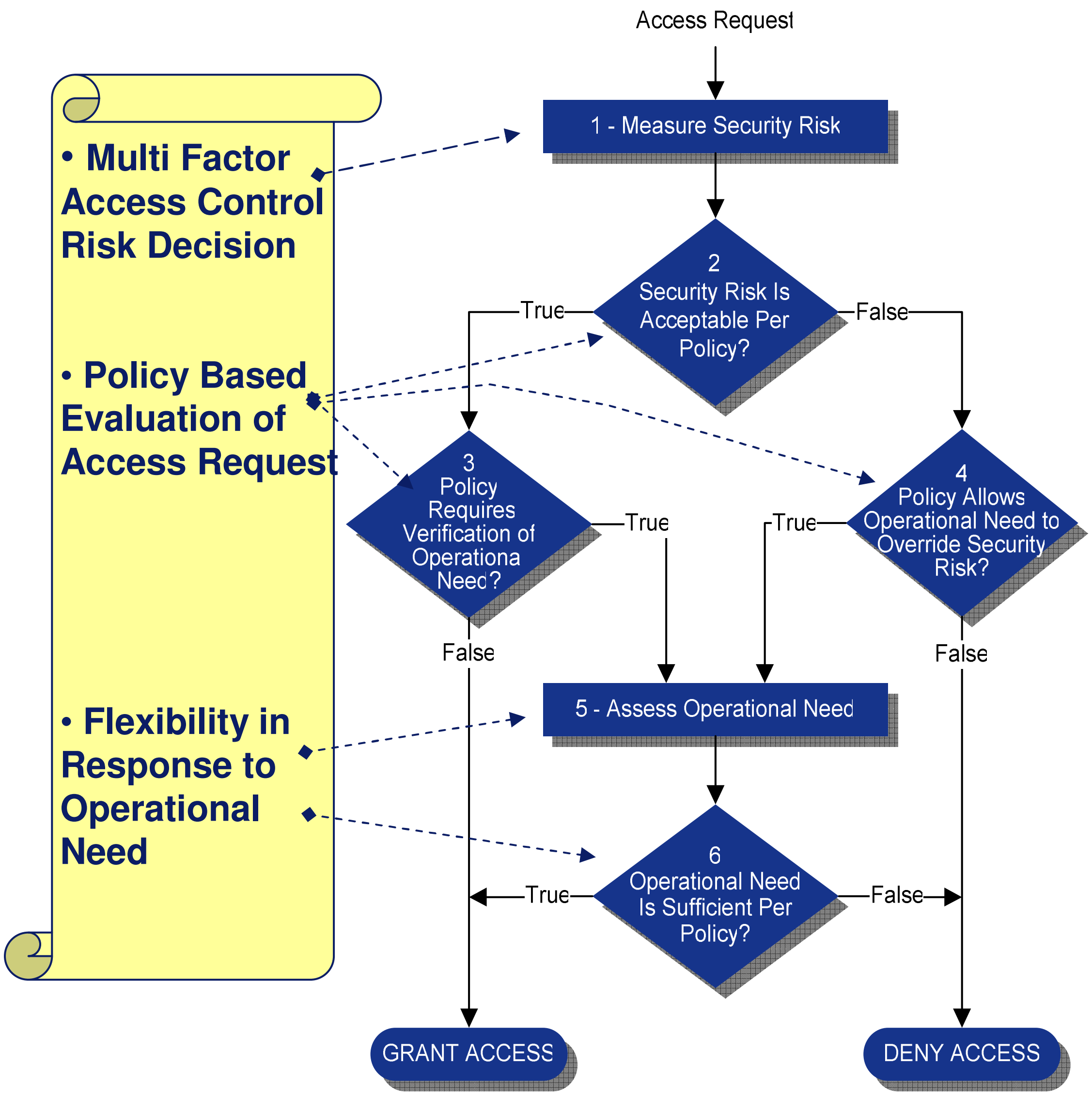
Access Control Decision - Traditional



- Object-level access control will become the primary protection mechanism for segregating information at different sensitivity levels
- Traditional access control approaches will not suffice to support the change in paradigm from need-to-know to need-to-share because they:
  - Demand satisfaction of clearance and need-to-know and assume that the risk of granting access is unacceptable if both are not met – no exception
  - Assume uniformity of people, IT components and situational conditions across the enterprise and time
  - Are inflexible

Access Control Decision – Risk and Policy Based

- A concept referred to as **R**isk **Ad**aptable **A**ccess **C**ontrol (RAdAC), is envisioned that will determine access based on:
  - The security risk in granting the access
  - Operational necessity for access
  - The enterprise’s policy for the balance between the two for various situations.
- Operational necessity can trump security risk
- Security risk is primarily a function of the people, IT components, content object being accessed, the environment in which they exist and historical access.
- Measurement of risk is envisioned to be done by ‘intelligent’ system processes, that will operate on a set of inputs and provide a risk level.



- **Multi Factor Access Control Risk Decision**
- **Policy Based Evaluation of Access Request**
- **Flexibility in Response to Operational Need**

Access Request

1 - Measure Security Risk

2 Security Risk Is Acceptable Per Policy?

True

False

3 Policy Requires Verification of Operationa Need?

True

False

4 Policy Allows Operational Need to Override Security Risk?

True

False

5 - Assess Operational Need

6 Operational Need Is Sufficient Per Policy?

True

False

GRANT ACCESS

DENY ACCESS

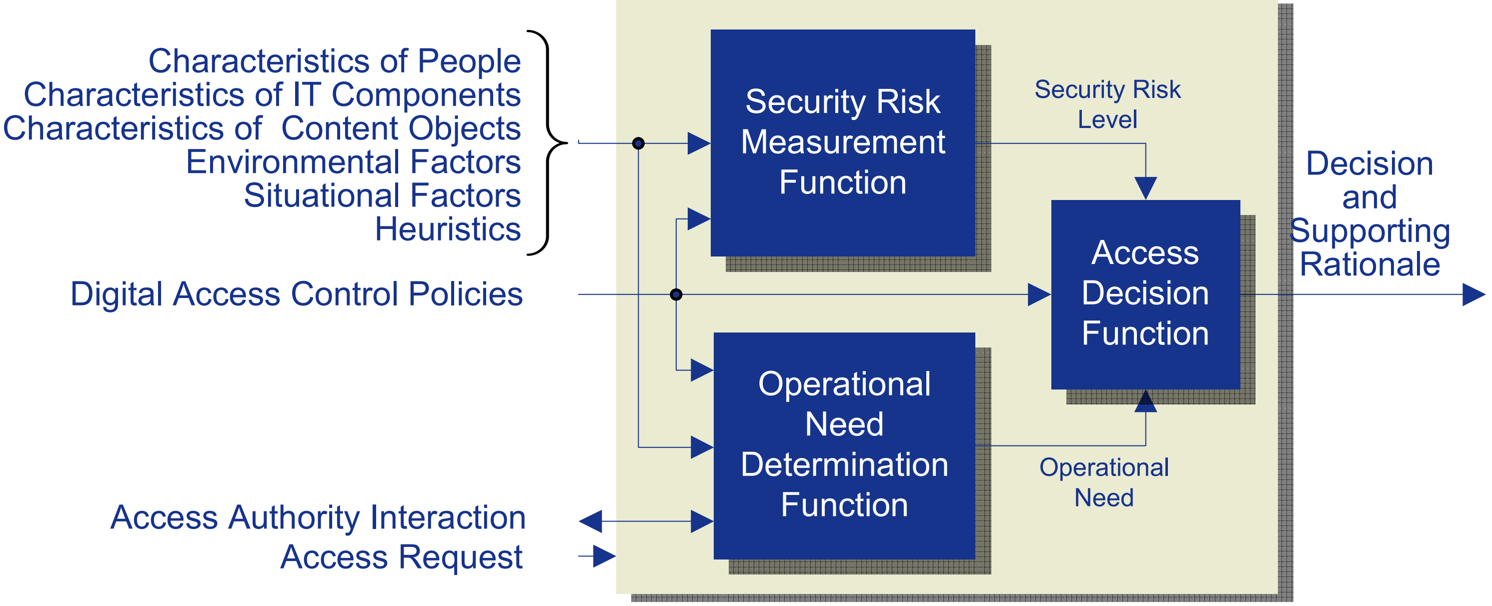
Access Control - Inputs

Characteristics of:

- The person (or other entity) to be given access
- The object or resource to be accessed
- The IT components involved and their pedigree
- The environment (e.g. location, facility) in which the person and IT components are operating

Other Inputs

- Situational Awareness (e.g. threat level condition)
- Heuristics – past decisions, knowledge of total enterprise risk
- Digital Access Control Policy – specifies levels of acceptable risk and required operational need



Characteristics of People
Characteristics of IT Components
Characteristics of Content Objects
Environmental Factors
Situational Factors
Heuristics

Digital Access Control Policies

Access Authority Interaction
Access Request

Security Risk Measurement Function

Security Risk Level

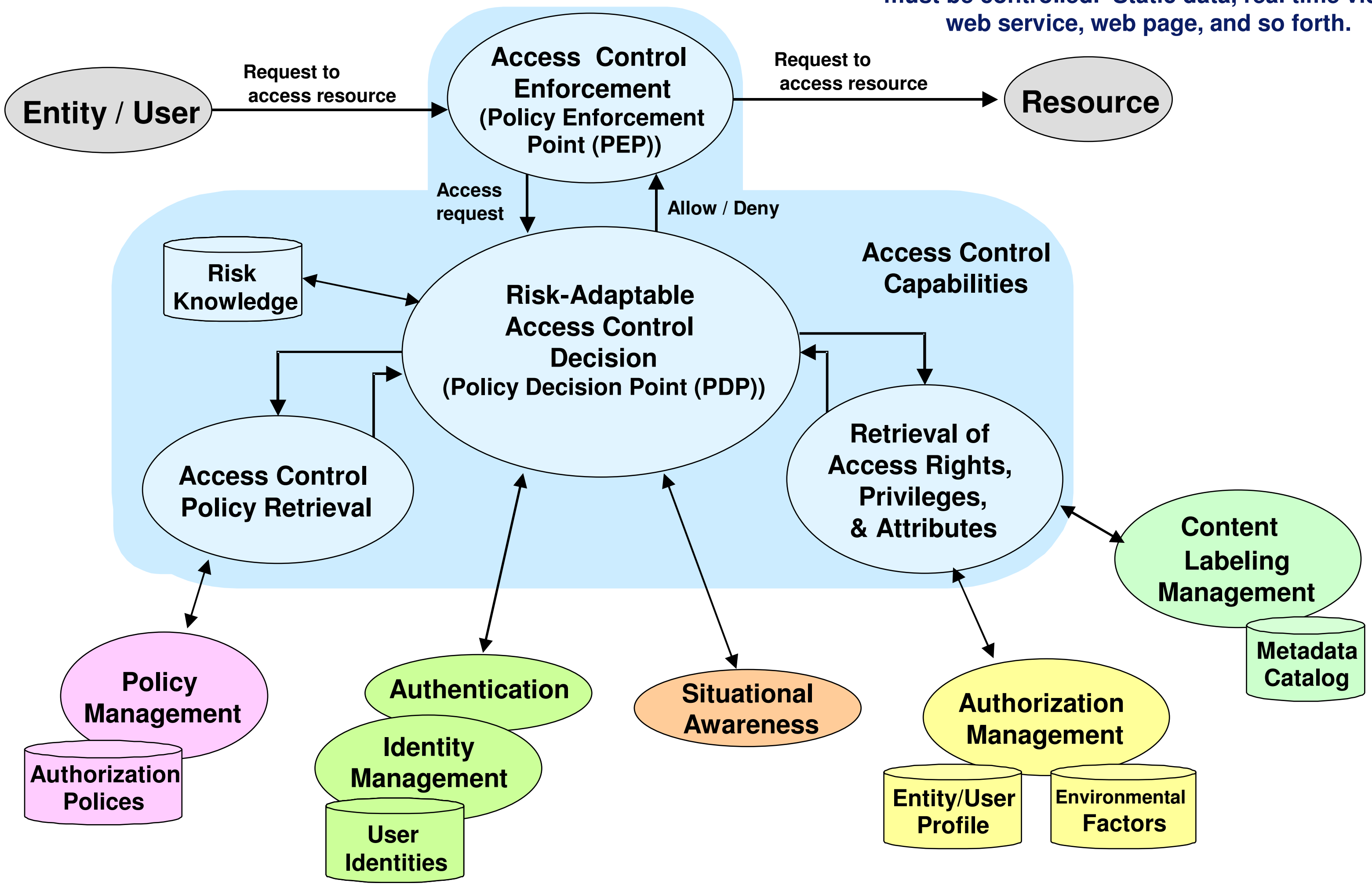
Access Decision Function

Operational Need Determination Function

Operational Need

Decision and Supporting Rationale

Access Control - Context


Entity / User
Request to access resource
Access Control Enforcement (Policy Enforcement Point (PEP))
Request to access resource
Resource
Access request
Allow / Deny
Access Control Capabilities
Risk Knowledge
Risk-Adaptable Access Control Decision (Policy Decision Point (PDP))
Access Control Policy Retrieval
Retrieval of Access Rights, Privileges, & Attributes
Content Labeling Management
Metadata Catalog
Policy Management
Authorization Polices
Authentication
Identity Management
User Identities
Situational Awareness
Authorization Management
Entity/User Profile
Environmental Factors

The access control enforcement would be distributed to various systems

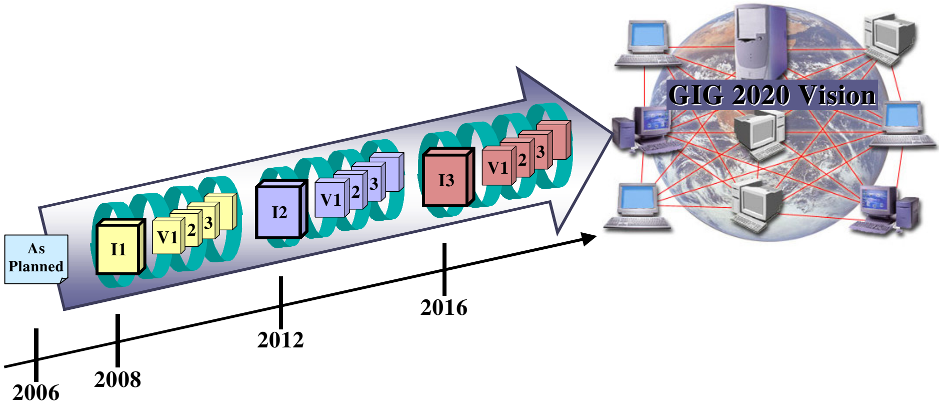
A resource could be any content to which access must be controlled. Static data, real time video, web service, web page, and so forth.

Some Technology and Research Challenges

- The whole Information Assurance vision for the evolution of the GIG is replete with technology and research topics.
- The access control concepts just discussed generate many. Here are a few:
  - Calculating security risk of access decisions – real time
  - Determining the affect of access decisions on overall enterprise security
  - Quantifying trust in people – through a security clearance or otherwise
  - Determining a person's operational need
  - Quantifying and calculating the level of trust for various identification and authentication mechanisms
  - Automatic determination and labeling of content protection requirements in accordance with enterprise policies, including subpart labels
  - Quantifying the trust level of IT components and systems.
  - Determining the location of IT components/client systems and quantifying the adversarial threat in that location
  - Heuristics as applied to access control decisions and improving access control decisions
  - Providing and managing digital security policies – dealing with conflict
  - Providing affordable, trustworthy components

Summary

- The DoD, via implementation of the Global Information Grid, is undergoing a transformation in the way it manages, communicates and secures its information content.
- Information Assurance is critical to the success of the GIG vision.
- The GIG will be realized through a phased implementation over 15+ years which:
  - Ensures Information Assurance capabilities, guidance, and policies exist to safely evolve to the next GIG increment
  - Ensures the transformation does not become so complex that it cannot be adequately understood and evaluated
- For more information on Information Assurance for the GIG, please visit the Information Assurance Technical Framework (IATF) Forum website at www.iatf.net.


GIG 2020 Vision
As Planned
I1
V1
2
3
I2
V1
2
3
I3
V1
2
3
2006
2008
2012
2016