Physical Access Control System (PACS) Evolution: Growing For The Future

Using the Enterprise Operations Management Analysis System (EOMAS) as a foundation for a "Next Generation" PACS

Developed in collaboration with SIA Standards and SIA Education by Bill Morgan, Avistas

Education | Government Relations | International Relations | Research & Technology | Standards

SIA
SECURITY
INDUSTRY
ASSOCIATION

Agenda

- **Federal Mandate for "Next Generation" PACS**

- **Identity, Credential, and Access Management (ICAM) adopted for Federal Use - FICAM**

- **FICAM leverages Security Industry Association's (SIA's) Open, Systems Integration and Performance Standards (OSIPS) Model**

- **Enterprise Operations Management & Analysis System (EOMAS) Introduction key to "Next Generation" PACS**

- **EOMAS Benefits**

- **EOMAS Framework**

- **Getting Started**

Education | Government Relations | International Relations | Research & Technology | Standards

635 Slaters Lane Suite 110 | Alexandria, VA 22314 | (866) 817-8888
www.siaonline.org

SIA
SECURITY
INDUSTRY
ASSOCIATION

The Mandate & The Response

May 2009,
White House Releases Cyberspace Policy Review
Federal Government Must Do More To Address Threats
Increase return on investment; Decrease Total Cost of Ownership

- **Identity, Credential, and Access Management (ICAM) efforts within the Federal Government are a key enabler for addressing the nation's security needs.**

- **Federal ICAM (FICAM) Goals, Published November 9th, 2009**
    - *Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM*
    - *Facilitate E-Government by Streamlining Access to Services*
    - *Improve Security Posture across the Federal Enterprise*
    - *Enable Trust and Interoperability*
    - *Reduce Costs and Increase Efficiency Associated with ICAM*
    - *Promotes forward looking objectives for: G2C, G2B and G2G*

- **FICAM Leverages Works of The Security Industry Association's (SIA) Standards Program**

Education | Government Relations | International Relations | Research & Technology | Standards

SIA
SECURITY
INDUSTRY
ASSOCIATION

Cloud Computing Transforms IT

State of Public Sector Cloud Computing

May 20, 2010

Vivek Kundra

Federal Chief Information Officer

Key Points:

- Services, not software
- Rent, don't buy
- Consolidate, don't duplicate

http://www.cio.gov/documents/StateOfCloudComputingReport-FINALv3_508.pdf

Economics Leads Policy

The Economic Gains of Cloud Computing

Vivek Kundra
Federal Chief Information Officer
www.whitehouse.gov
April 7, 2010

Key Points:

- "Cloud-first" policy
- Data center consolidation
- Centralize certification
- Establish Standards

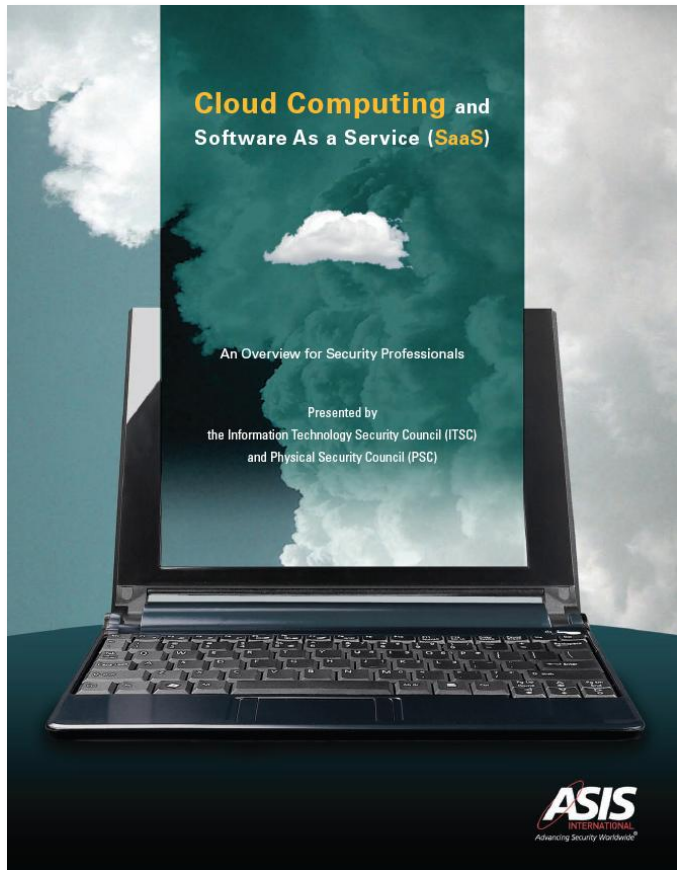http://www.brookings.edu/~/media/Files/events/2010/0407_cloud_computing/0407_cloud_computing_kundra_presentation.pdf

Education | Government Relations | International Relations | Research & Technology | Standards

635 Slaters Lane Suite 110 | Alexandria, VA 22314 | (866) 817-8888
www.siaonline.org

SIA
SECURITY
INDUSTRY
ASSOCIATION

Physical Security Adopts Tenants of the Cloud

Cloud Computing and Software As a Service (SaaS)

An Overview for Security Professionals

Presented by
the Information Technology Security Council (ITSC)
and Physical Security Council (PSC)

ASIS INTERNATIONAL
Advancing Security Worldwide

http://www.asisonline.org/councils/documents/CloudComputingFinal.pdf

Applications Available As Cloud Services:

- Access Control
- Intrusion
- Video Surveillance
- Detection
- Visitor Management
- Mass Notification

Drivers:

- Economics
- Efficiency

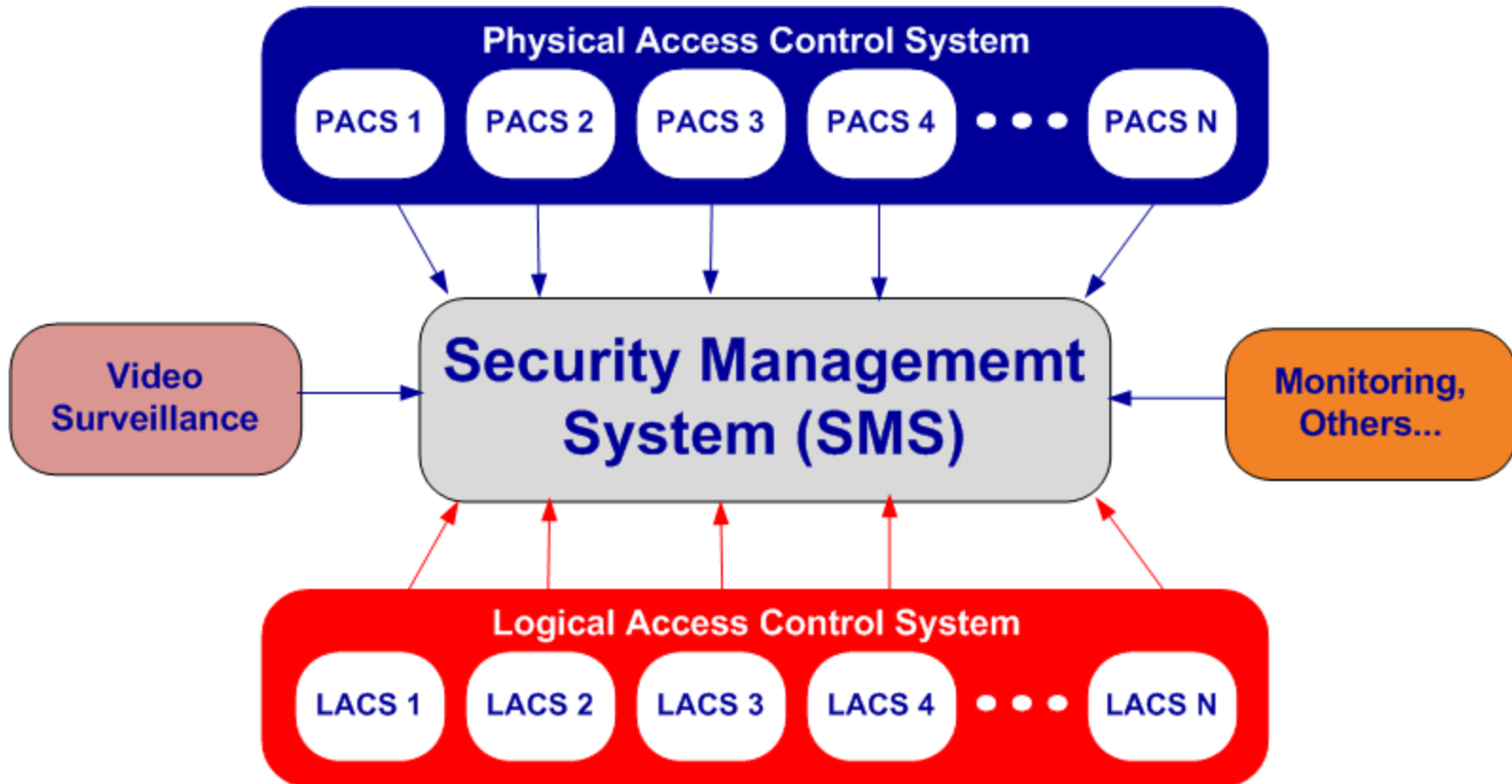**Education | Government Relations | International Relations | Research & Technology | Standards**

635 Slaters Lane Suite 110 | Alexandria, VA 22314 | (866) 817-8888
www.siaonline.org

SIA
SECURITY
INDUSTRY
ASSOCIATION

Today's Security Management System
Interfacing PACS, LACS, Video, Monitoring...

Physical Access Control System

PACS 1 | PACS 2 | PACS 3 | PACS 4 | • • • | PACS N

Video Surveillance → **Security Managememt System (SMS)** ← **Monitoring, Others...**

Logical Access Control System

LACS 1 | LACS 2 | LACS 3 | LACS 4 | • • • | LACS N

Education | Government Relations | International Relations | Research & Technology | Standards

SIA's Contributions to FICAM
Introduces The Enterprise Operations, Management, and Analysis System Concept

- *SIA Published "Applying OSIPS to ICAM" – An Application White Paper*

  - OSIPS – Open, Systems Integration and Performance Standards – A family of SIA Standards

  - Traditional PACS and LACS roles were reduced to services that provisioned and defined PACS and LACS access privileges used by access points they control

  - ICAM recognized that the federal PACS, LACS, and SMS should evolve into what some have called an *Enterprise Operations, Management and Analysis System (EOMAS)*

- *An EOMAS provides the maximum integration, interoperability and performance of FICAM assets from the field, edge, middleware and core components*

- *EOMAS scales by Group, Division, Agency and Department to achieve FICAM goals and operates from within the cloud*

- *A properly designed EOMAS harmonizes the information associations between different subsystems leveraging the value of all of the enterprise assets.*

SIA
SECURITY INDUSTRY ASSOCIATION

Enterprise Operations Management & Analysis Systems (EOMAS)
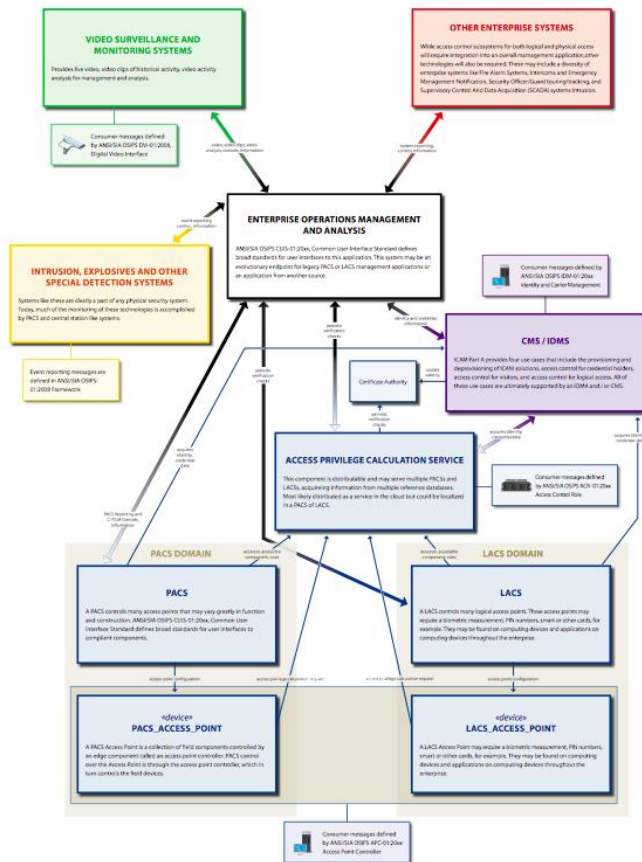
EOMAS leverages OSIPS Architecture for Enterprise Interconnectivity of Next Generation PACS:

- VIDEO SURVEILLANCE AND MONITORING SYSTEMS
- INTRUSION, EXPLOSIVES AND OTHER SPECIAL DETECTION SYSTEMS
- ENTERPRISE SYSTEMS (GIS, Asset Management, HR, Business Intelligence, etc.)
- CMS / IDMS
- ACCESS PRIVILEGE CALCULATION SERVICE
- PACS DOMAIN
- PACS_ACCESS_POINT
- LACS DOMAIN
- LACS_ACCESS_POINT

Architectural details are described in -
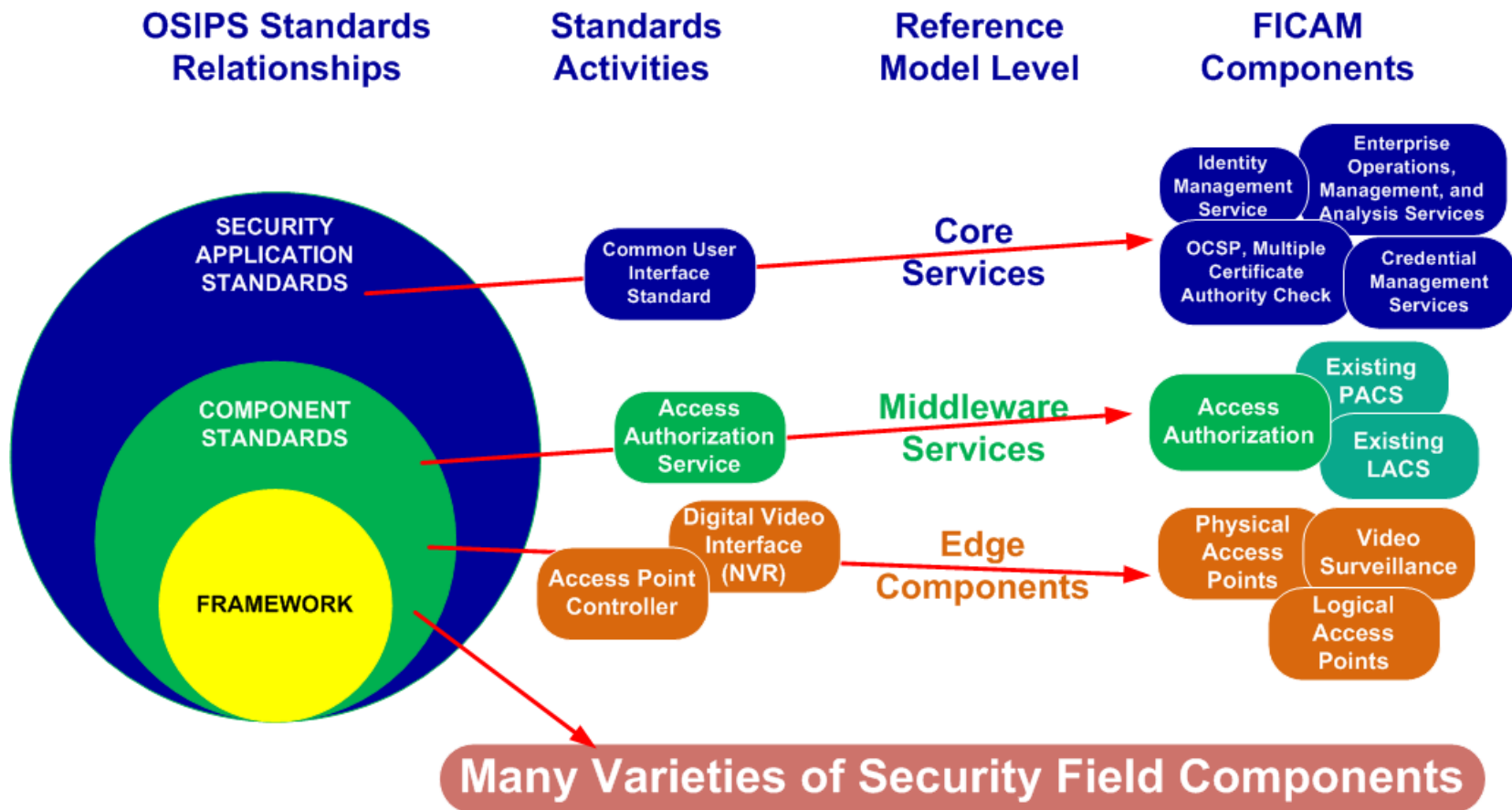
"Applying OSIPS to ICAM" – An Application Whitepaper

http://www.siaonline.org/WorkArea/showcontent.aspx?id=7108

Education | Government Relations | International Relations | Research & Technology | Standards

OSIPS Architecture, Activities, Reference Model, and ICAM

OSIPS Standards Relationships

- SECURITY APPLICATION STANDARDS
- COMPONENT STANDARDS
- FRAMEWORK

Standards Activities

- Common User Interface Standard
- Access Authorization Service
- Digital Video Interface (NVR)
- Access Point Controller

Reference Model Level

- Core Services
- Middleware Services
- Edge Components

FICAM Components

- Identity Management Service
- Enterprise Operations, Management, and Analysis Services
- OCSP, Multiple Certificate Authority Check
- Credential Management Services
- Access Authorization
- Existing PACS
- Existing LACS
- Physical Access Points
- Video Surveillance
- Logical Access Points

Many Varieties of Security Field Components

Education | Government Relations | International Relations | Research & Technology | Standards

SIA
SECURITY INDUSTRY ASSOCIATION

OSIPS Reference Model –
Core Services Components
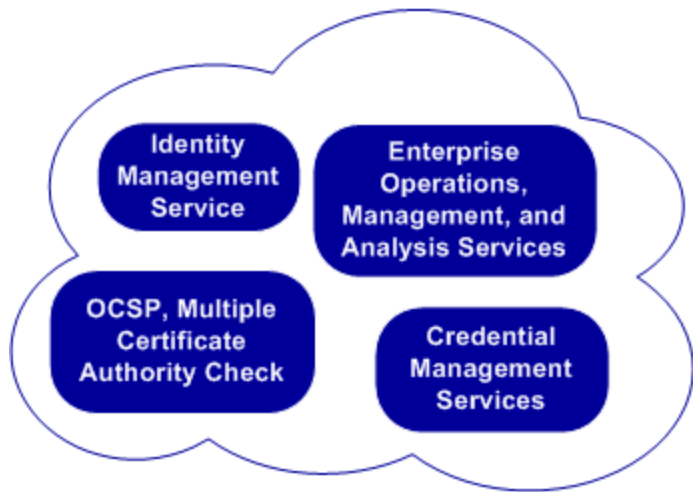
- The Core Services Components provide critical services such as central data storage, identity management systems, and credential management systems.

- These applications usually operate on powerful servers located at the core of the enterprise's computational infrastructure, including public or private clouds.

- These core components provide essential information for middleware applications like Access Authorization Services, Legacy PACS and LACS, and edge components such as Access Points that have a need to relate directly to them.

OSIPS Reference Model –
Middleware Application Components
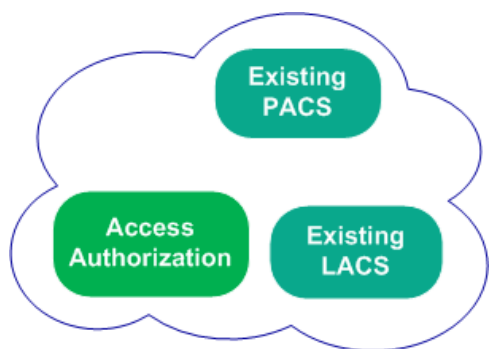
- Middleware Application Components appear more frequently than core components within the system architecture and provide distributable points of concentration between core components of any system and the many edge components with which they must interact.

- In OSIPS, middleware components:
  - Serve as "Front-end" management components that control distributed collections of edge components like PACS or LACS
  - concentrate communications from collections of edge components to core components like caching certificates and performing certificate authentication
  - provide support for special applications not practical for operation within core components
  - act as an efficient mechanism for peer-to-peer communications between edge components.

Existing PACS

Access Authorization

Existing LACS

Education | Government Relations | International Relations | Research & Technology | Standards

SIA
SECURITY
INDUSTRY
ASSOCIATION

635 Slaters Lane Suite 110 | Alexandria, VA 22314 | (866) 817-8888
www.siaonline.org

OSIPS Reference Model
Edge Components

Physical Access Points

Video Surveillance

Logical Access Points

- **Edge Components provide the applications that monitor and control the actual physical world of the enterprise.**

- **This is the system layer that provides the connection between the software representation of the system and the hundreds or thousands of field components that are visible to users of the system.**

- **Edge Components are software applications residing in edge devices that provide the specialized, communications ports needed to interact with their field components including: TCP/IP, RS485, ModBus, BACnet, DeviceNet, SAML, HTTP(S), SOAP and many more.**

- **Edge Components are typically serviced and managed by cloud-based applications that provide provisioning and enforce mission specific policies. For an access point this might be an Access Authorization Service, a PACS, or LACS.**
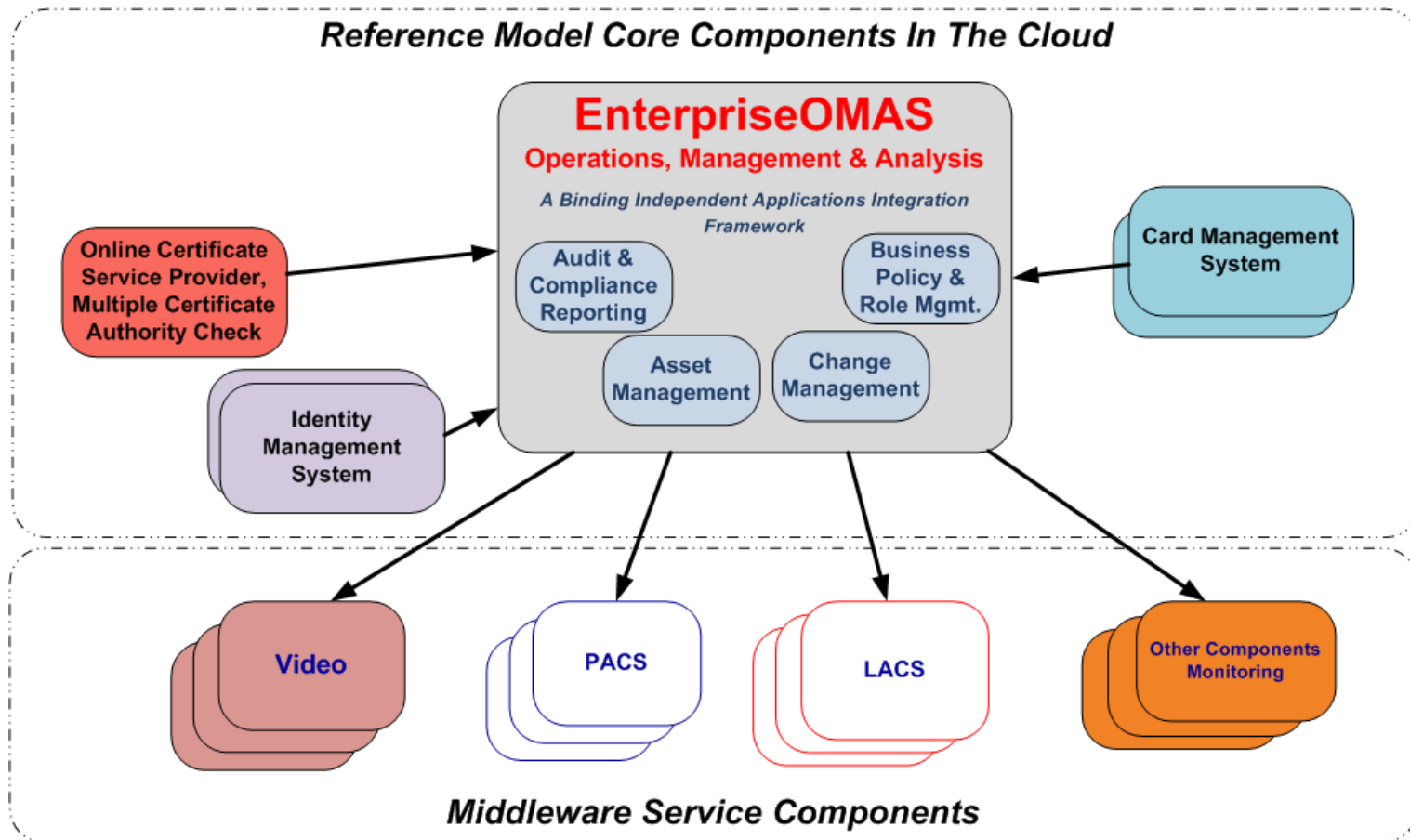
Education | Government Relations | International Relations | Research & Technology | Standards

635 Slaters Lane Suite 110 | Alexandria, VA 22314 | (866) 817-8888
www.siaonline.org

SIA
SECURITY
INDUSTRY
ASSOCIATION

OSIPS Reference Model
Field Components

Physical Access Points

Logical Access Points

Video Surveillance

- **Field Components, of which there are thousands in any enterprise system, include such things as door sensors, gate operators, signaling lights, locks, temperature sensors, flow meters, intercom and phone stations, card readers, cameras, D/NVRs, and thousands of other devices and instrumentation.**

- **These physical assets must be well maintained, managed and carefully monitored with tight administrative and change management controls.**

SIA
SECURITY
INDUSTRY
ASSOCIATION

OSIPS Reference Model and Enterprise OMAS

Reference Model Core Components In The Cloud

EnterpriseOMAS
Operations, Management & Analysis

A Binding Independent Applications Integration Framework

- Audit & Compliance Reporting
- Business Policy & Role Mgmt.
- Asset Management
- Change Management

Online Certificate Service Provider, Multiple Certificate Authority Check

Identity Management System

Card Management System

SECURITY MANAGEMENT SYSTEM

Video | PACS | LACS | Other Components Monitoring

Middleware Service Components

Education | Government Relations | International Relations | Research & Technology | Standards

SIA
SECURITY
INDUSTRY
ASSOCIATION

Other Major EOMAS Architecture Benefits

- **Quantifies FICAM Goal Attainment**
- **Facilitates Real-time (or near real-time) Line-of-Sight**
- **Enables Multi-vendor interoperability**
- **Enables Multi-protocol interoperability**
- **Leverages Cloud Services**
- **Leverages Core Components**
- **Preserves Separation of Duties**
- **Preserves Defense in Depth**
- **Rules-based Configurations Assure Compliance**
- **Provides Audit Trails**
- **Provides Alarms, Alerts & Reporting**
- **Assures Integrity of PACS Assets**
- **Facilitates Change Management for PACS Assets**

SIA
SECURITY
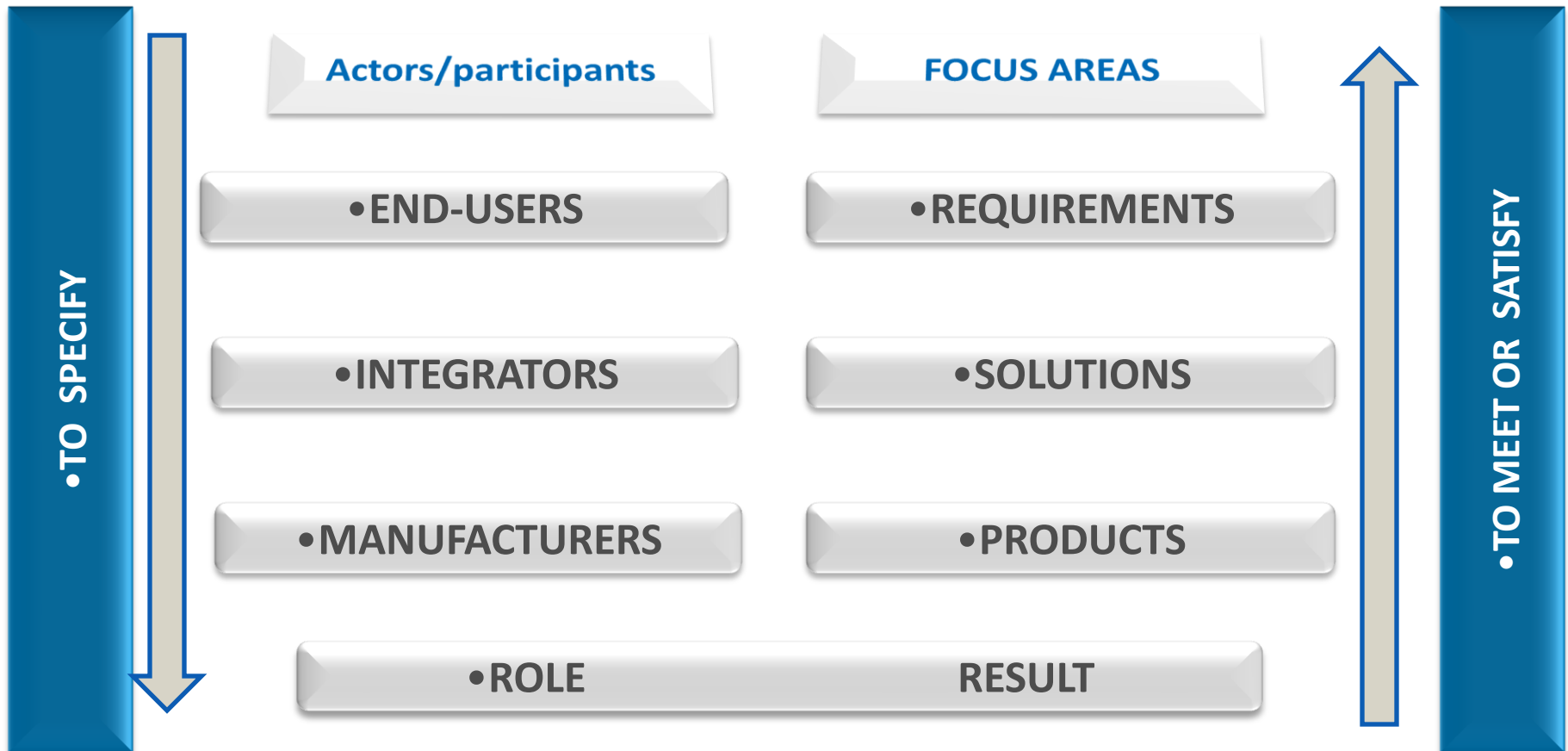INDUSTRY
ASSOCIATION

Business Objectives Of EOMAS*

- Increased security, which correlates directly to reduction in identity theft, data breaches, and trust violations. Specifically, ICAM closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing.

- Compliance with laws, regulations, and standards as well as resolution of issues highlighted in GAO reports of agency progress.

- Improved interoperability, specifically between agencies using their PIV credentials along with other PIV-interoperable or third party credentials that meet the requirements of the federal trust framework. Additional benefits include minimizing the number of credentials requiring lifecycle management.

- Enhanced customer service, both within agencies and with their business partners and constituents. Specifically, secure, streamlined, and user-friendly transactions translate directly into improved customer service scores, lower help desk costs, and increased consumer confidence in agency services.

- Elimination of redundancy, both through agency consolidation of processes and workflow and the provision of government-wide services to support ICAM processes. This results in extensibility of the IT enterprise and reduction in the overall cost of security infrastructure.

- Increase in protection of personally identifiable information (PII) by consolidating and securing identity data, which is accomplished by locating identity data, improving access controls, proliferating use of encryption, and automating provisioning processes.

Aligns with "Federal Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance" document published November 10th, 2009 – Executive Summary, page ii
http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

Education | Government Relations | International Relations | Research & Technology | Standards

SIA
SECURITY INDUSTRY ASSOCIATION

OSIPS Framework Implementation

Actors/participants	FOCUS AREAS
•END-USERS	•REQUIREMENTS
•INTEGRATORS	•SOLUTIONS
•MANUFACTURERS	•PRODUCTS
•ROLE	RESULT

•TO SPECIFY

•TO MEET OR SATISFY

•**OSIPS Framework is a business-case driven standard that is applicable to end-users, integrators/solution providers and manufacturers/developers**

Education | Government Relations | International Relations | Research & Technology | Standards

SIA
SECURITY
INDUSTRY
ASSOCIATION

How To Design An EOMAS
Identify and Link Functional Building Blocks and Services

An Enterprise Is A Collection Of Functions Performed By Employees Filling Roles Using Information Produced By Enterprise Technologies And Services

Enterprise Employee Roles

- CEO, CFO, etc.
- Executive Management
- Division Management
- Department Management
- Supervisors
- Mission Worker

An Enterprise Function or Service

(Mission Profile w/ Metrics)

Actionable Information Feeds

- Real-time Status Information On Workstations, PDAs, etc.
- Summary Activity Reports By E-Mail, Printed Reports, Inquiry
- Alert Messages By PDA, Text Message, MMS
- Actionable Business Intelligence Adapted to Every Worker's Role

1 - Inventory the functions of your enterprise including the employee roles, required information, and required information sources

Essential Information Comes From Enterprise Systems

- Access Control
- Video Surveillance
- Infrastructure Monitoring and Control
- SCADA Monitoring and Control
- Facilities & Energy Management
- Human Resources
- Change Management
- Performance Management
- Asset Management
- Risk Management
- Audit & Compliance

Education | Government Relations | International Relations | Research & Technology | Standards

SIA
SECURITY INDUSTRY ASSOCIATION

How To Design An EOMAS
Determine How Subsystems Are Used

For a specific technology, each supported function requires...

Federal — **Assurance**

Subordinate Agency / Organization — **Compliance**

Major Operational Unit — **Policies**

Operational Sub-Unit — **Practices**

Supervisor — **BI**

Worker — **Auth & Access**

...information that is presented in actionable format so that the authorized employees, contractors and guests performing those functions by role, may successfully perform their duties and tasks for all related enterprise services.

FICAM Services & Next Generation PACS

2 – Accumulate all *Application Requirements* for each employee role for each enterprise service component.
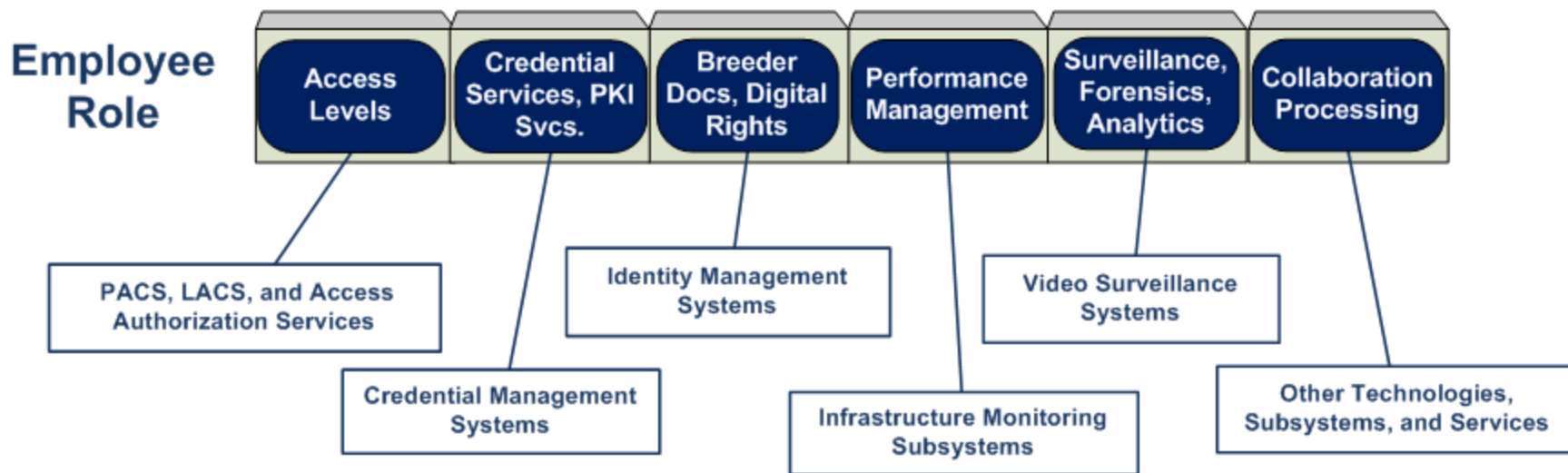
Application Requirements

- **Define the Mission**
- **Define the Goals**
- **Define the Roles of All Stakeholders**
- **Identify Required Resources**
- **Define Operational Requirements**
- **Define the Performance Requirements**
- **Establish Quality Controls**
- **Identify Internal Dependencies**
- **Identify External Dependencies**
- **Identify Risks**
- **Define Budgets**
- **Define Timelines**

Education | Government Relations | International Relations | Research & Technology | Standards

SIA SECURITY INDUSTRY ASSOCIATION

Harmonize Information Associations
Leverage Employee Roles Across the Enterprise

3 – Leverage employee roles by associating functions from many enterprise components into a useable interface for each.

Employees depend on information from several enterprise technology components, services and workflows.

Employee Role

| Access Levels | Credential Services, PKI Svcs. | Breeder Docs, Digital Rights | Performance Management | Surveillance, Forensics, Analytics | Collaboration Processing |

PACS, LACS, and Access Authorization Services

Identity Management Systems

Video Surveillance Systems

Credential Management Systems

Infrastructure Monitoring Subsystems

Other Technologies, Subsystems, and Services

Education | Government Relations | International Relations | Research & Technology | Standards

SIA
SECURITY INDUSTRY ASSOCIATION

Put The Enterprise Operations, Management, and Analysis System Together
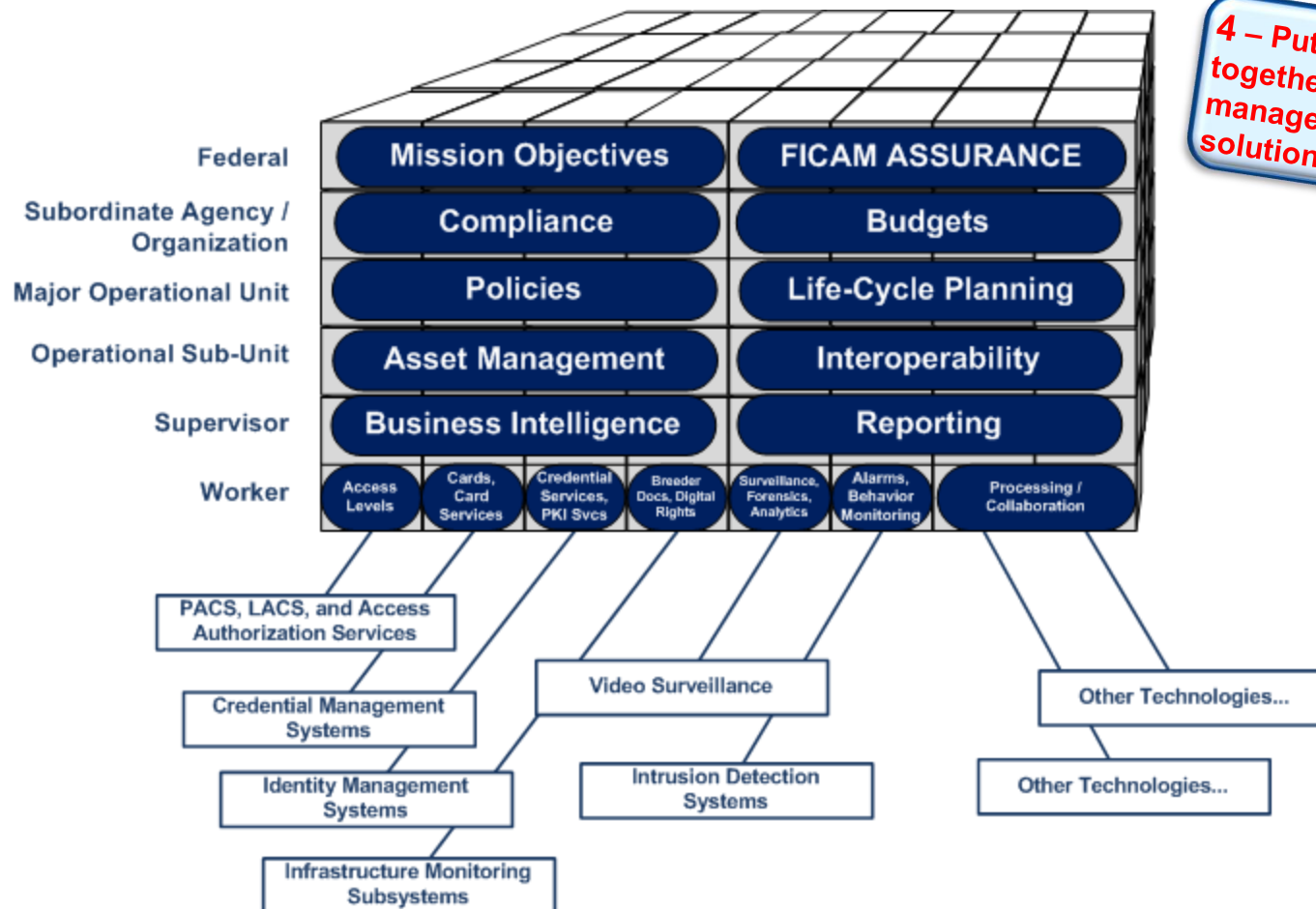
4 – Put the enterprise functions together to define the operations, management, and analysis solution.

Education | Government Relations | International Relations | Research & Technology | Standards

Additional Resources

Identity, Credentialing and Access Management Road Map

http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

http://www.idmanagement.gov/documents/ICAM_Roadmap_Snapshot.pdf

"Applying OSIPS to ICAM" – An Application Whitepaper

http://www.siaonline.org/WorkArea/showcontent.aspx?id=7108

Standards Activities

http://www.siaonline.org/landing.aspx?id=1524&linkidentifier=id&itemid=1524

Additional Questions:

Joe Gittens (jgittens@siaonline.org)

703-647-8486

Bill Morgan (bmorgan@avistas.com)

214-544-0400

Education | Government Relations | International Relations | Research & Technology | Standards

SIA
SECURITY
INDUSTRY
ASSOCIATION