Enterprise Management Solutions Protection Profiles

Eric Winterton, Booz | Allen| Hamilton
Joshua Brickman, CA Inc.

September 2008

Agenda

- Protection Profiles what do we have now
- Defining Enterprise Security Management
- Requirements being demanded by government agencies
- The gap? How close are we?
- A Solution
- Q and A

Current State of Protection Profiles

- PP’s currently support the following technologies:
  - Access Control Devices/Systems
  - Boundary Protection Devices and Systems
  - Data Protection
  - Databases
  - Detection Devices/Systems
  - IC’s and Smart Card Devices/Systems
  - Key Management
  - Network and Network related Devices/Systems
  - Operating Systems
  - Products for Digital Signatures
  - Other Devices/Systems

Current State of Protection Profiles

- **We are addressing the following technologies:**
  - **Access Control Devices/Systems**
  - **Boundary Protection Devices and Systems**
  - **Data Protection**
  - **Databases**
  - **Detection Devices/Systems**
  - **IC's and Smart Card Devices/Systems**
  - **Key Management**
  - **Network and Network related Devices/Systems**
  - **Operating Systems**
  - **Products for Digital Signatures**
  - **Other Devices/Systems**

What is Enterprise Security Management?

- Enterprise services critical security functions include:
  - Multilevel Access Control Solutions
  - Single sign on
  - Centralized Monitoring and Response
  - Standardized Auditing
  - Centralized Configuration and Compliance
  - Integration into existing architectures (data import & export)
  - Automated provisioning with workflow approval process
- Various PP’s help achieve these goals individually but they are not mutually inclusive.

Current CC Environment for ESM Products

- Custom Security Targets
- Longer and more costly evaluations
- No Apples to Apples to compare for customer
- Moratorium (NIAP) limits and restricts ability of Vendors to quickly provide software to demanding Federal customers with US Evaluation

Current State of IT Security

- Security systems and processes are fragmented
- Risk is higher than ever (internal and external)
- Demands are higher than ever from:
  - Business
  - Customers
  - Partners
  - Government and Auditors

Enterprise Management Challenges

USERS

- Fast, 24/7 app access
- Good user experience
- Secure data
- Reduce my logons

RISK

- Secure app access
- Protect systems, resources
- Right access to the right person
- Manage, remediate vulnerabilities

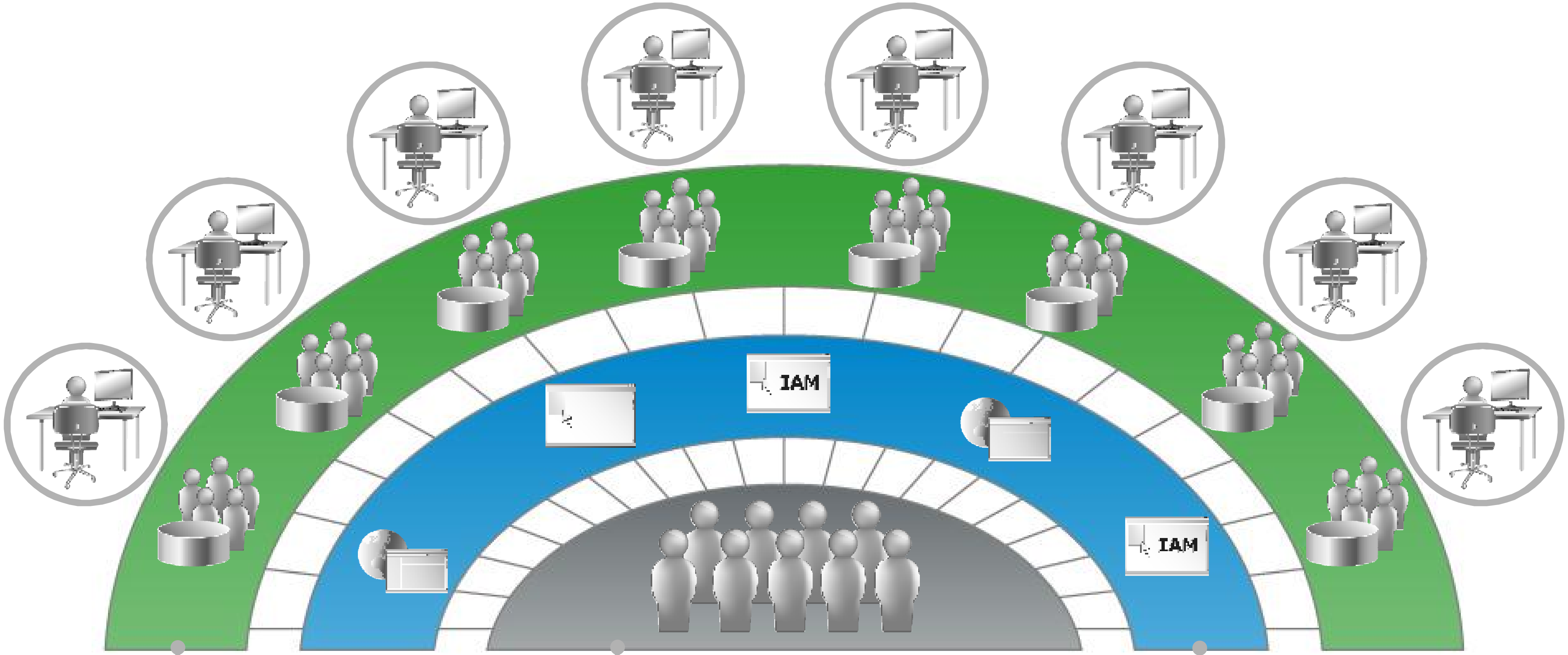
BUSINESS

- Deploy more apps
- Integrate more partners
- Support more customers
- Integrate acquisitions
- Do it faster/cheaper
- Avoid bad press

REGULATORY

- Continuous compliance
- Strong internal IT controls
- Privacy of customer information
- Document processes and controls

The Identity Challenge



MANY IDENTITIES

- Mainframe
- RDBMS
- LDAP
- NOS
- ERP...

MANY USERS

- Customers
- Employees
- Partners

MANY APPLICATIONS

- Logistics
- Financial
- Service
- Production
- CRM
- ERP

General Issues faced by Federal Agencies

National Institute of Standards and Technology

NIST

...working with industry to foster innovation, trade, security and jobs

Common Criteria

IPA® 独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

nis National Intelligence Service | ITSCC

Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

Canadä

Français	Contact Us	Help	Search	Canada Site
Home	National Security	Privacy & Accountability	ITS Program	History
About CSEC	Public Info	Publications	Careers	Site Map

THE COMMON CRITERIA EVALUATION AND VALIDATION SCHEME

National Security

ca Booz | Allen | Hamilton

General Issues faced by Federal Entities

> Many governing directives and laws; FISMA, NIST, DoD 8500.x, FIPS, IPV6, Section 508 (VPATS), FDCC, HSPD-x, HIPAA, CCTM, TEMPEST, CTCPEC, ACSI 33, etc

> High expectations from citizens and users for IT availability, credibility, security and industry leading technology

> Support changes in staff, leadership, fiscal directions and organizational priorities

> Highest threat environment for IT at any point in history

Specific Issues and Threats

- > Managing User Accounts From the Beginning to End of Their Life Cycle
- > Securing Vital Information by Enforcing Access Policies and Protecting the Data
- > Meet Regulatory Requirements for Auditing and Reporting
- > Keep the "Bad Guys" Out and Still Provide Superior Customer Service
- > Stay "Future Proof" – Technology That Stays Current

The Destination

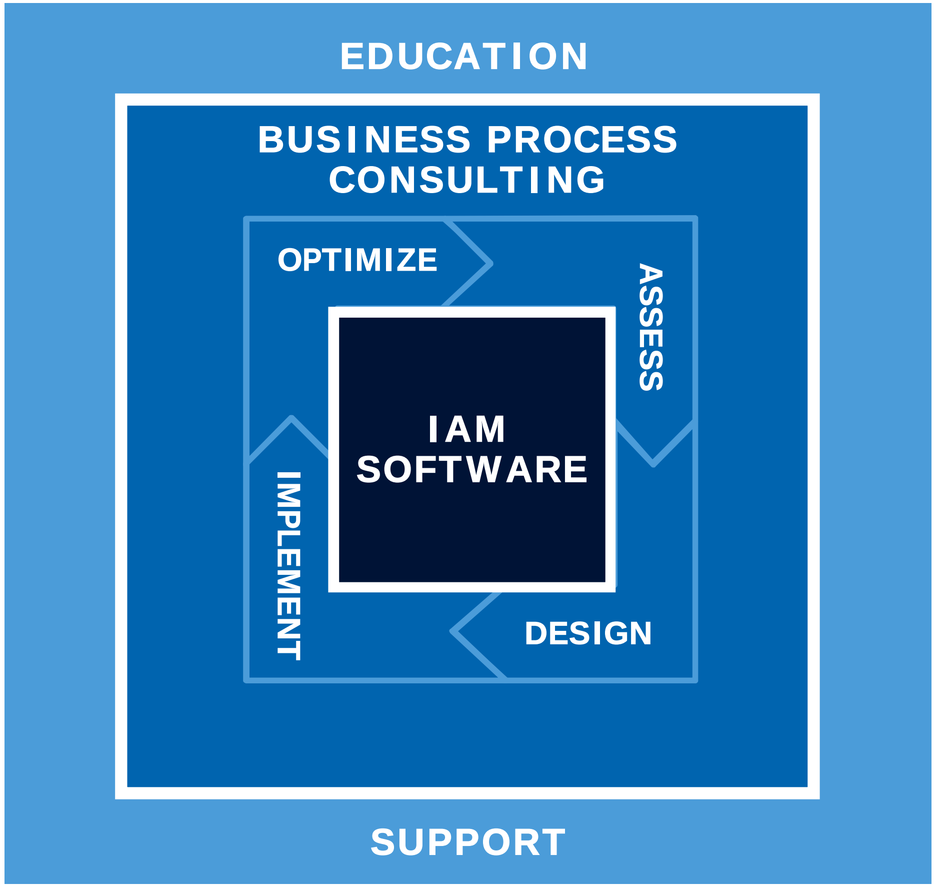
The Interactive e-Government

- Applications & Transactions
- Content & Information
- Community & Collaboration

Citizens
Customers
Partners
Employees

To provide secure, interactive access to all required resources for every e-Government relationship

Identity and Access Management



SOFTWARE

SERVICES

EDUCATION AND SUPPORT

A COMPLETE SOLUTION TO MEET FEDERAL GOVERNMENT REQUIREMENTS

Identity & Access Management Delivers

- > **Reduced IT Security Risk**
  - § Protect your critical data and resources
  - § Centrally manage all identities, lifecycles and access policies
- > **Reduced Operational Expenses**
  - § Lower your IT Admin and Help Desk expenses
  - § Automate existing manual IT processes
- > **Enhanced Compliance**
  - § Controls automation provides provable compliance
  - § Help achieve your governance, risk & compliance goals
- > **Enhanced Business Enablement**
  - § Deploy new online services quickly and securely
  - § Strengthen your existing customer relationships

Reduced IT Security Risk

> Key Technology Requirements:

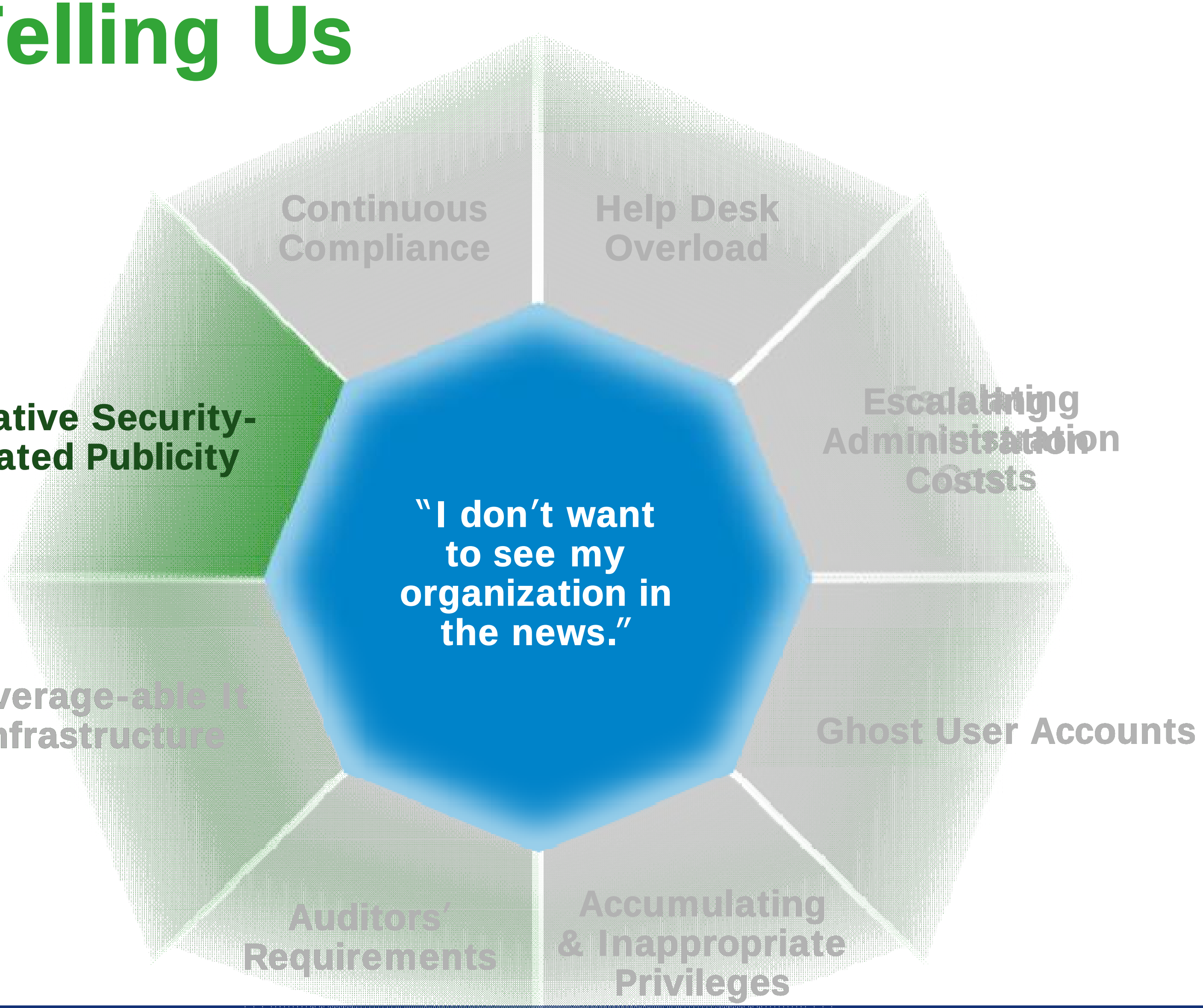
- Centralized policy and role-based access management for:
  - Web applications
  - Systems and platform resources
  - Critical system services (e.g., auditing process)
  - Web Services
  - Mainframes
- Granular superuser access entitlements
- Auditing of all user access events
  - Filtering & correlation of event info to help identify security issues

Reduction of Operational Expenses Through Automation

> Key Technology Requirements:

- § Reduced administration expenses
  - – Centralized management of all user identities and access policies
  - – Automated (de-)provisioning of accounts and access rights
  - – Automated filtering and correlation of all security event info
  - – Delegated management of users
- § Reduced help desk costs
  - – Single sign-on across all applications
  - – User self-service
- § Improved productivity of users & managers
  - – Automated provisioning with workflow approval process

What CIOs, CSOs and CFOs Are Telling Us



Continuous Compliance

Help Desk Overload

Escalating Administration Costs

Ghost User Accounts

Accumulating & Inappropriate Privileges

Auditors' Requirements

Leverage-able It Infrastructure

Negative Security-Related Publicity

"I don't want to see my organization in the news."

Protection Profiles That Come Close

- Protection Profile Authorization Server for Basic Robustness Environments [U.S.]
- Discretionary Information Flow Control (MU) [Germany]
- Controlled Access Protection Profile [U.S.]
- Protection Profile for a Identity Manager [Germany]
- Protection Profile Intrusion Detection System - System for Basic Robustness Environments [U.S.]

We need aspects of these protection profiles but each of them has some difficulty meeting the entire set of requirements for ESM.

...So just how close are we?

A Solution

- Start with a base PP using minimal requirements and build upon those functions for more complex ESM functionality.
- Using some existing PP's as templates we create a new family of PP's for ESM.
- Multiple EAL's for various needs of customers and vendors.
- Work with the various schemes, vendors and customer communities to build the PP's.

The Outcome

- True Apples to Apples comparison: making COTS acquisitions easier and faster for agencies
- Side effect of encouraging COTS vendors to add features to meet PP’s, thus meeting the requirements of the customers
- Faster and cheaper evaluations of PP compliant applications

So how can you help?

- CA and Booz are committed to participating in this effort but we cannot do it alone.
  - Vendors/customers: Participate in requirements gathering
  - Schemes: Accept and validate this approach
  - Other interested parties: we welcome your help!

- Your comments and feedback are encouraged!

Eric Winterton, CISSP
CCTL Technical Director
Booz | Allen | Hamilton
Linthicum, MD USA
+1-410-684-6691
winterton_eric@bah.com

Joshua Brickman
Program Manager, Federal Certifications
CA, Inc.
Framingham, MA USA
+1-508-628-8917
Joshua.Brickman@ca.com