Challenges to Ensuring Secure Dot-COM and Dot-EDU Web Access

June 19, 2003

Standards-Based Architecture Program Office

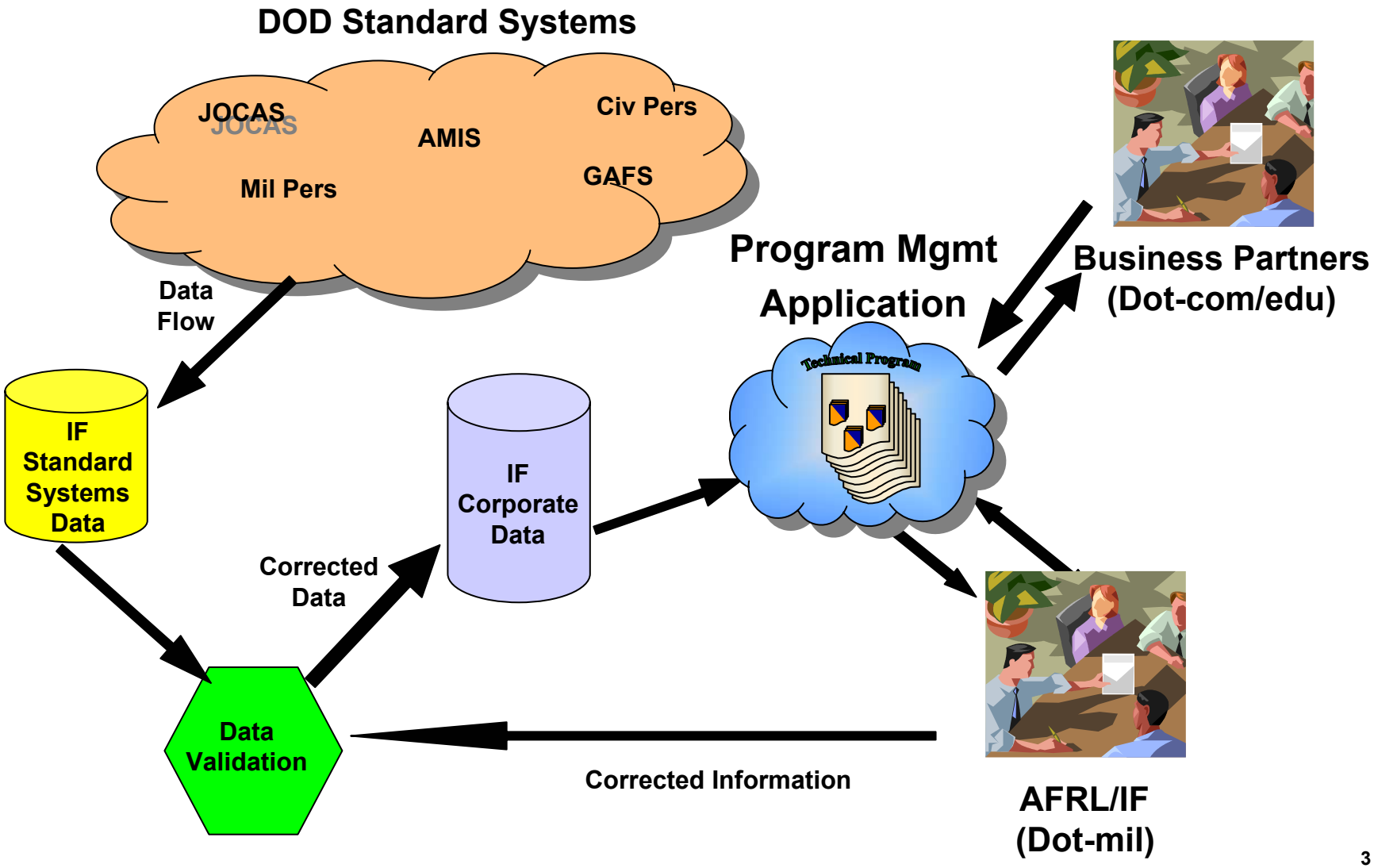
Information Directorate

Air Force Research Laboratory

System Information

- Web Based Tool Built Primarily for Post Award Contract Management
- Designed for a Distributed Work Environment
- Contractor Financial and Technical Reporting
- Government Sharing of Program Management Info
- One Way Data Feeds from Corporate Database (Data Entered Once)
- Data entry is almost entirely web based and validated against AFRL corporate data
- Goal is to make contract reporting quick and easy and provide access to needed effort or program information.

Information Strategy

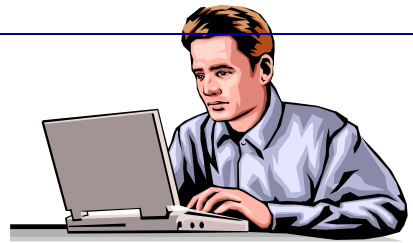


Tailored User Information

Dot-mil Users

Dot-com/edu Users

Buyer



LPM

LPM Support

Super User

Financial Administrator

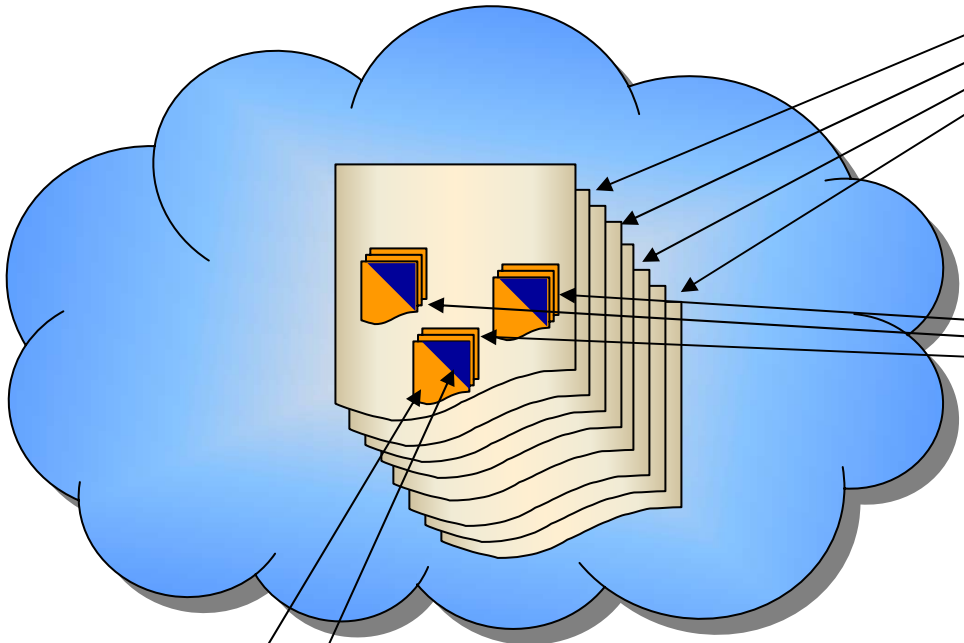
Other Technical

Principal Investigator (PI)

PI Support

Data Compartmenting

- **Application accounts are limited by the User's Programs, Projects And Permission Level.**



Programs

- Collaboration
- Non-collaboration

Projects

- Contracts
- In-House
- Working Groups

Data Access

- Government Only
- Govt and Contractor

Permission Levels

- 5 possible levels

User Management

- User Agreements
  - Verify identity
  - Agree to Rules
- Secure Passwords
- Delegated Authority
  - Local Super Users
  - Govt POCs
  - Contractor POCs
- Automatic Permission Assignments
- Audit Trails
  - User Traceability
  - Security Reports

Add / Edit

All Program Functions/People

All Project Functions/People

Some Project Functions/People

Who did What to Whom and When

and

Who can see What since When

Account Generation Procedure

Existing App user

Nominates person

System generates Confirmation Code for new account

Confirmation Code given to Nominee

Verbal Identification and Confirmation Code given to Help Desk

Nominee

Login and change temporary password

Begin Using System

Fill out electronic Account Agreement

Print out, get signatures, fax Account Agreement to Help Desk

Help Desk

User ID, Temporary Password, System URL sent to Nominee

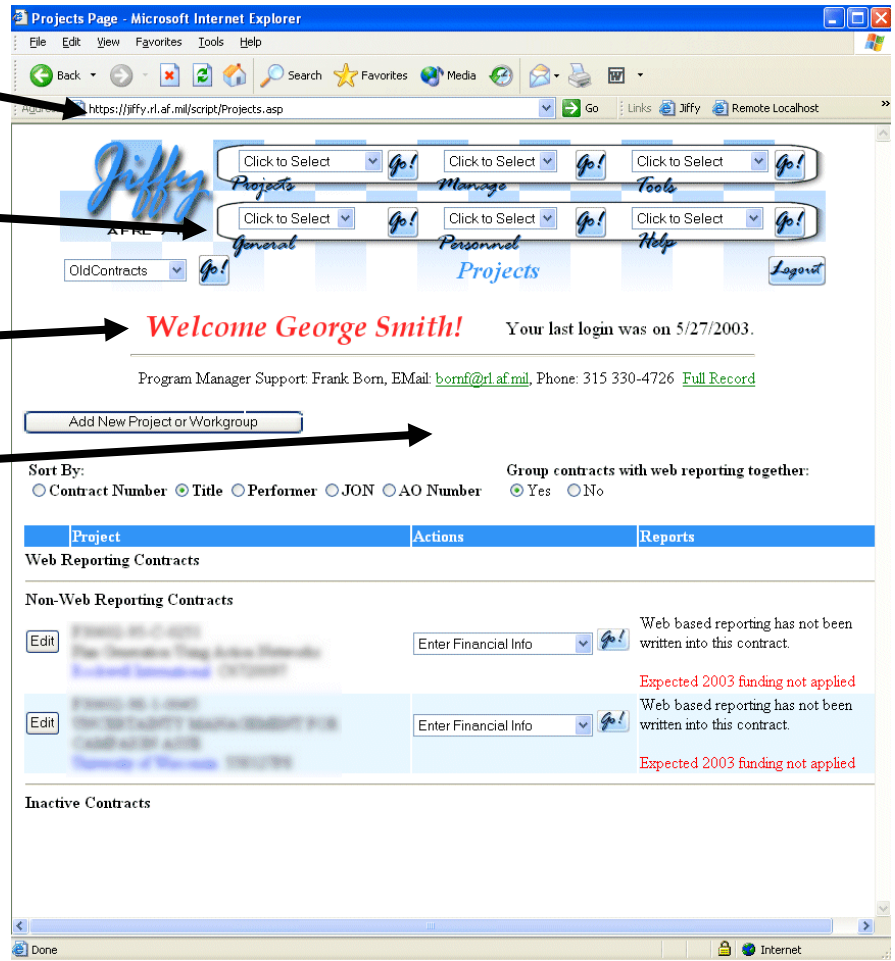
Email Notification of Valid User Account Creation to Nominee

Review Account Agreement

Activate User Account

Page Security

- Disabled URL editing
- Permission Level / Program Tailored Navigation Bars
- Server based User Authentication
- Page Level Permission Checks
- Session Timeouts
- Session Logout



Additional Security Measures

- Web server not a member of the domain
- Secure Socket Layer
- 128 bit encryption
- File name obscurity

https://PMSys.af.mil/Documents/Program/DCF10/ISI_2-0576(Le+G1Rpvvic2T)7.htm