

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**



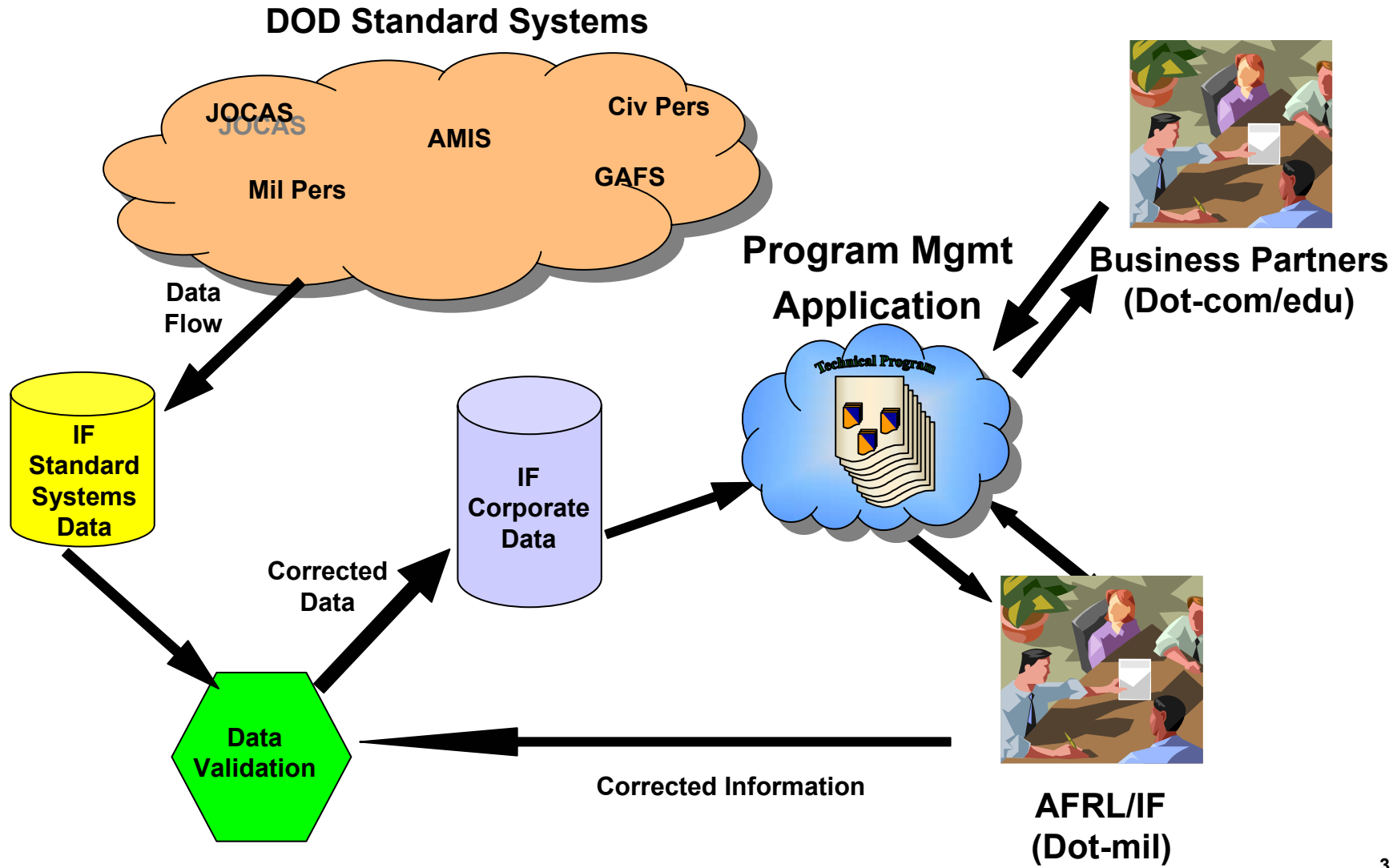
System Information



- **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

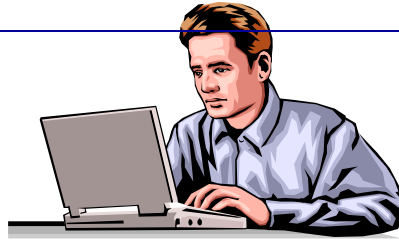


Dot-mil Users

Dot-com/edu Users



Buyer



LPM



LPM Support



Super User



Other Technical



Principal Investigator (PI)



Financial Administrator

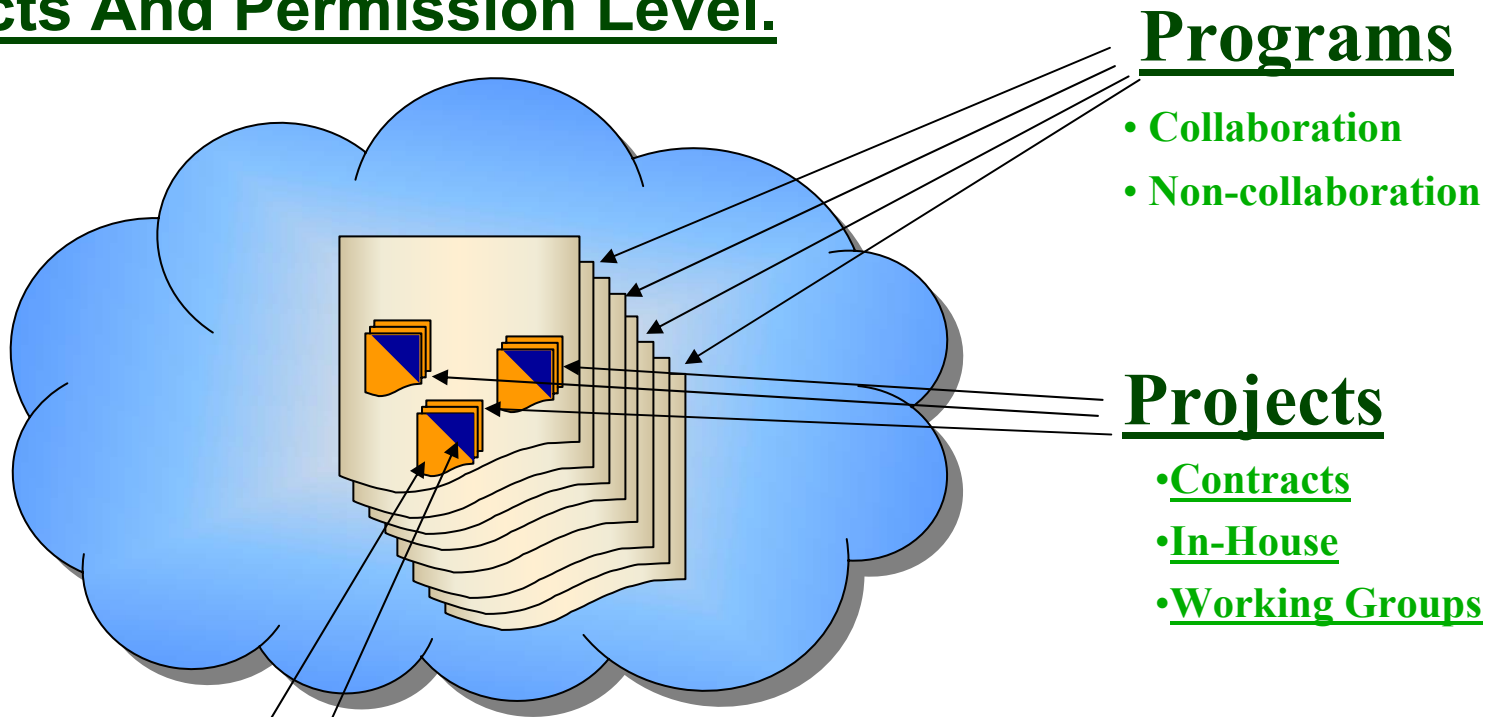


PI Support



Data Compartmenting

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



Data Access

- Government Only
- Govt and Contractor



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

The screenshot shows a 'User Agreement' form with the following sections:

- User Information:** Name, SSN, Company, Address, Phone, Fax, E-mail, and User ID.
- Confirmation:** Confirmation No. and Confirmation Date.
- Agreement:** A section with checkboxes for 'I have read and agree to comply with all the information contained in this user agreement document' and 'I will be held responsible for any misuse of the system for which I am a user of the system and I will be held liable for any damage caused by my misuse of the system'.
- Signature:** A line for the user's signature and a line for the system administrator's signature.
- Date:** A line for the date of the agreement.
- Approval:** A line for the approval of the system administrator.

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



System generates
Confirmation Code
Nominates person
for new account

Confirmation
Code given to
Nominee



Nominee



Login and change
Begin Using System
Fill out electronic
password
Account Agreement
Print out, get
signatures, fax
Account
Agreement to Help
Desk

Verbal Identification
and Confirmation
Code given to Help
Desk



User ID, Temporary
Password, System
Email Notification of
URL used to Account
Creation to Nominee

Review Account
Agreement
Activate User Account

Help Desk





Page Security



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

The screenshot shows a Microsoft Internet Explorer window titled "Projects Page - Microsoft Internet Explorer". The address bar shows the URL "https://jiffy.rl.af.mil/script/Projects.asp". The page content includes a navigation bar with "Click to Select" dropdowns and "Go!" buttons for categories like "Projects", "Manage", "Tools", "General", "Personnel", and "Help". A user welcome message reads "Welcome George Smith! Your last login was on 5/27/2003." Below this is a "Program Manager Support" section with contact information for Frank Born. A table of contracts is displayed, with columns for "Project", "Actions", and "Reports". The table is divided into "Web Reporting Contracts", "Non-Web Reporting Contracts", and "Inactive Contracts".

Project	Actions	Reports
Web Reporting Contracts		
Non-Web Reporting Contracts		
[Edit] [Contract Info]	[Enter Financial Info] [Go!]	Web based reporting has not been written into this contract.
[Edit] [Contract Info]	[Enter Financial Info] [Go!]	Expected 2003 funding not applied Web based reporting has not been written into this contract.
Inactive Contracts		



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