Project Title: Annual Security Inventory (ASI) Application

Submitted By

David Gracey
Deputy CIO, Enterprise Solutions - University of California, Riverside
david.gracey@ucr.edu
951-827-7367

Team Members

Sumita Roy-Chowdhury, Primary Application Developer
Brandon Ayers, Application Architect
Jeremy Fisher, Technical Infrastructure Lead

Project Summary

The Annual Security Inventory (ASI) application was developed to more effectively manage the inventory of sensitive information stored and processed on computer systems across campus. Documenting the institution's electronic information resources allows the campus to identify areas of risk, determine where additional security measures are needed, and ensure compliance with University of California information security policies and standards.

Project Narrative

Prior to implementing the ASI application, campus IT departments were required to fill out standalone documents and send via email their security plans, system names, and IP addresses of systems containing sensitive data to the responsible administrative official and the central IT organization (Information Technology Solutions). The emails were then archived for later retrieval and review in the event an audit was needed, or a system was compromised. The goal of the Annual Security Inventory project was to improve the way this information is gathered, organized, stored, and retrieved.

The previous, email-based solution for managing the security inventory was fraught with issues. Some departments did a good job of reporting the sensitive information contained within their computer systems and the security controls in place. Others provided incomplete or inconsistent information at best. There was a desire to improve both the quality of the information being provided by individual campus IT organizations as well as central oversight to ensure complete and accurate inventories were being provided consistently across the institution.

A centralized database and corresponding web-based application was designed to capture the relevant information security details for each campus system including, but not limited to, the types of protected data contained therein (e.g. Social Security Number, Driver's License Number, Credit Card Number), whether each data element is encrypted, whether physical and host-based security measures are in place, information about database and file system access controls, details about system backups and disaster recovery plans, and so on. Business rules were implemented within the application to avoid incomplete submissions. Logic was added to ensure all required questions are answered and valid values are selected for each data field. System roles and workflows were implemented to ensure the report for each system or environment is entered by the department, reviewed by the organization, routed to Information Technology Solutions for final review, and ultimately approved.

The ASI application had a positive impact on customers. The user experience features a simple and easy-to-navigate interface, stepping the user through the data collection process for each of their computer systems. For convenience, each year's inventory is pre-populated based upon the reports submitted the previous year. This allows departments to focus on specifying what is new, what has changed, and what no longer exists rather than the busywork of re-entering a lot of the same or similar information year after year.

UCR's Chief Information Security Officer indicates the ASI application is much easier and more convenient to use than completing the security inventory on email or paper. Historical data can be referenced to populate current year's security inventory which accelerated completing the survey. The Information Security Office has the functionality to provide suggestions and remediation guidelines on completed assessments to assist clients with improving their security posture. The application has integrated routing from department to organization, to Information Security Office making it a more efficient workflow. Several UC campuses including Santa Barbara, Santa Cruz, and Berkeley have shown interest in using the ASI application considering there is an appreciation for the work to have the application be multitenant.

The success of the project is measured by the accuracy and completeness of the Annual Security Inventory. Reports were built within the system to reveal which reports have been submitted by which campus departments, and which reports are still pending. This allows the Information Security Office to engage with campus units as needed to ensure 100% compliance with reporting requirements including adherence to BFB-IS-3 University of California policy for electronic information security.

The ASI application has broken-down silos between campus IT organizations. There is now a free flow of information security data across the institution.

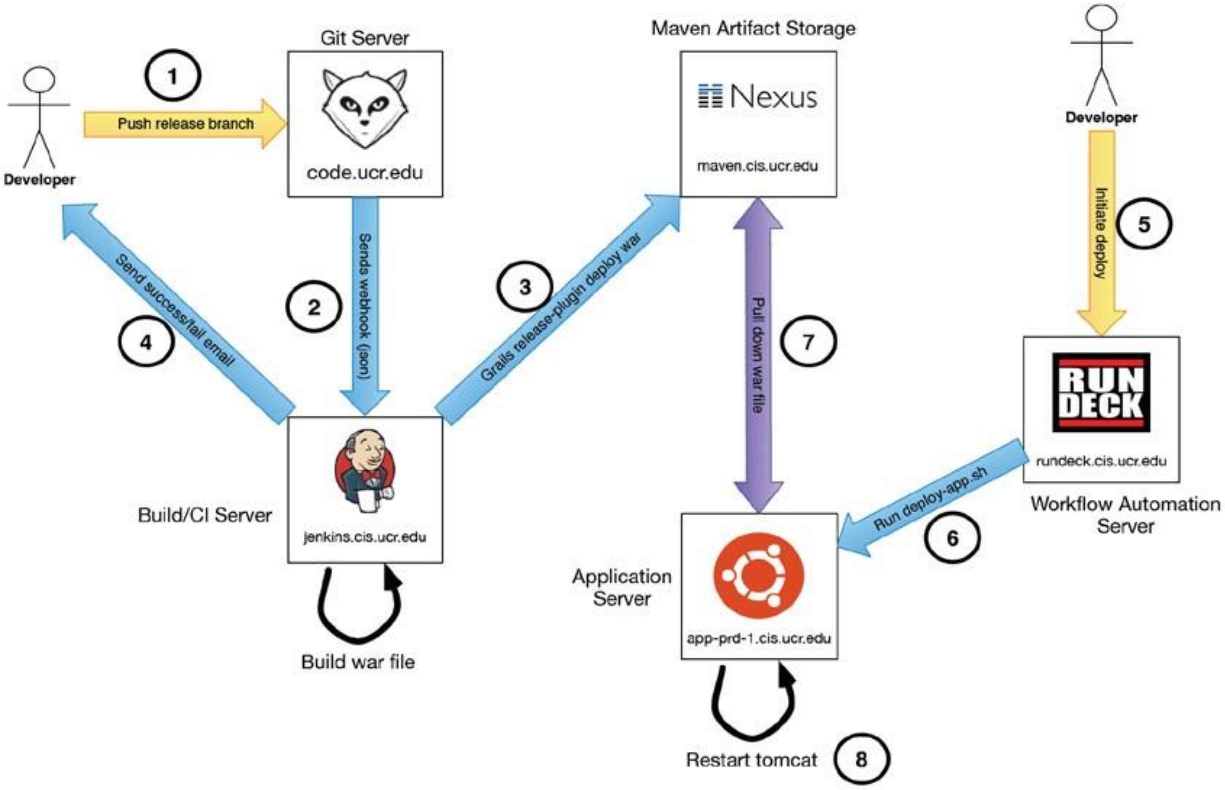
Project Timeline

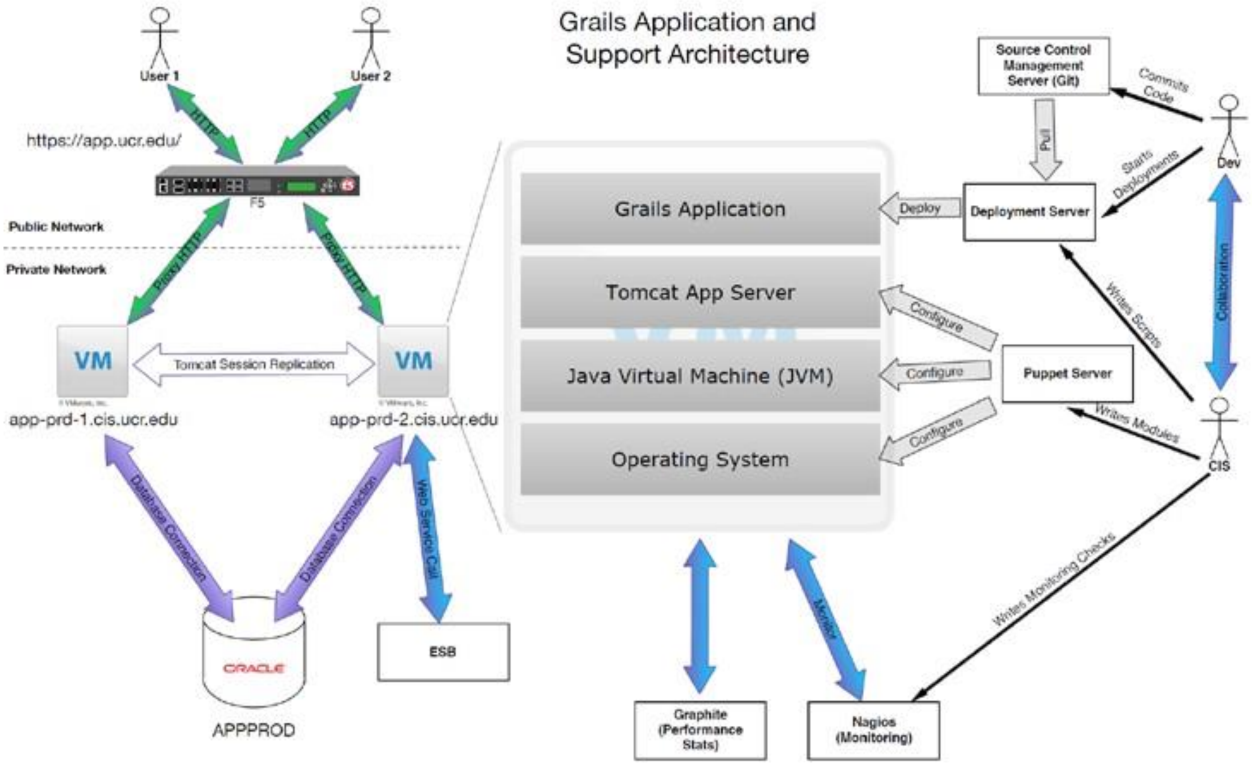
September 2015	Planning and Design
October 2015	Development
November 2015	Testing and Deployment
July 2018	Update to support policy BFB-IS-3: Electronic Information Security
January 2019	Multi-Tenancy Architecture Review
August 2019	Application Hosting for Additional UC Campus Locations

Technology Highlights

- Architected to host multiple tenants.
- ASI uses Single Sign-on (CAS) for authentication and the campus Enterprise Access Control System (EACS) for authorization.
- ASI is built with GRAILS. The GRAILS (Groovy on Rails) programming language and technology stack. This high-productivity development framework enables UCR to build web applications like ASI in a very short timeframe.
- It is built for Mobile platforms. ASI implementation is developed with Responsive Web Design. Thus, it is mobile-friendly and optimized for various mobile devices (e.g., tablets, smartphones).
- Common Infrastructure. ASI leverages existing infrastructure (e.g., virtual machines, storage, and database) thereby allowing developers to focus on development and not on back-end configuration details.
- ASI takes advantage of a suite of application development tools that allows for rapid development.
  - The GRAILS (Groovy on Rails) programming language and technology stack
  - Development IDE supporting Java, and Model View Controller (MVC)
  - Common infrastructure (e.g., virtual machines, storage, and database)
  - Puppet to automatically provision Virtual Machines
  - Jenkins to create new builds
  - Rundeck for deployment
  - Apache Fuse Enterprise Service Bus (ESB) to provide web service integration for:
    - User authorization
    - Person information
    - Accountability structure (orgs and depts.)
  - Responsive design allowing the application to resize itself dynamically for optimal display regardless of device
  - ASI leverages existing infrastructure (e.g., virtual machines, storage, and database) allowing developers to focus on development and not on backend configuration details

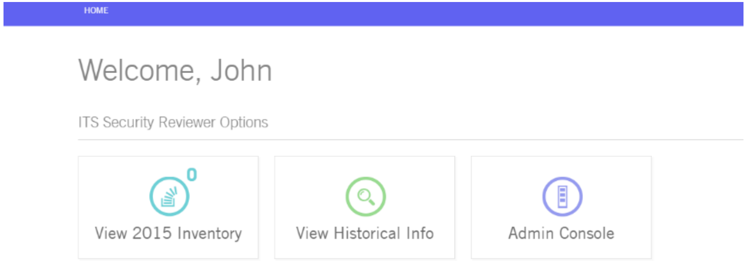
Build and Development Process




Grails Application and Support Architecture
User 1
User 2
HTTP
HTTP
https://app.ucr.edu/
F5
Public Network
Private Network
Proxy HTTP
Proxy HTTP
VM
Tomcat Session Replication
VM
app-prd-1.cis.ucr.edu
app-prd-2.cis.ucr.edu
Database Connection
Database Connection
Web Service Call
ORACLE
APPPROD
ESB
Grails Application
Tomcat App Server
Java Virtual Machine (JVM)
Operating System
Source Control Management Server (Git)
Commits Code
Pull
Starts Deployments
Dev
Deploy
Deployment Server
Collaboration
Configure
Configure
Configure
Puppet Server
Writes Scripts
Writes Modules
CIS
Writes Monitoring Checks
Monitor
Graphite (Performance Stats)
Nagios (Monitoring)

ASI Screen-Shots

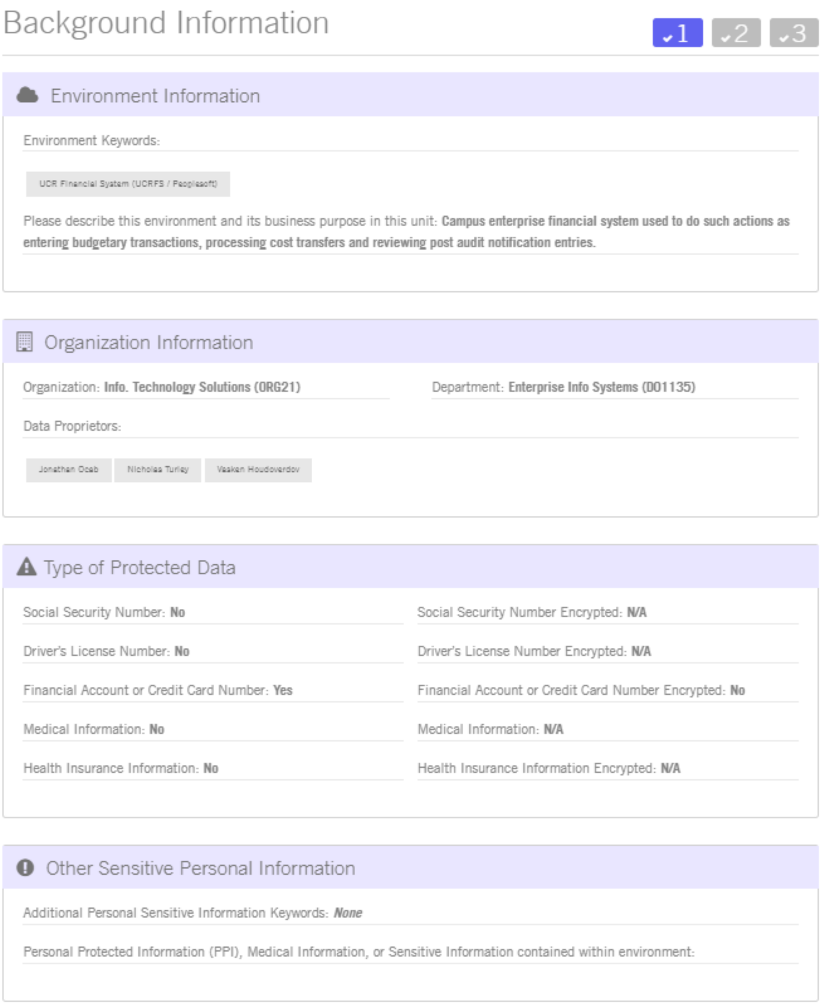
Main Menu dynamically presents tiles corresponding to the user’s authorizations (the illustration below shows options for the application administrator):



Welcome, John

ITS Security Reviewer Options

The application guides the user through the process of gathering required information for each system (page 1):



Background Information

Environment Information

Environment Keywords:

UCR Financial System (UCRFS / Peoplesoft)

Please describe this environment and its business purpose in this unit: **Campus enterprise financial system used to do such actions as entering budgetary transactions, processing cost transfers and reviewing post audit notification entries.**

Organization Information

Organization: **Info. Technology Solutions (ORG21)**

Department: **Enterprise Info Systems (D01135)**

Data Proprietors:

Jonathan Ocab

Nicholas Turley

Vaskan Houdoverdov

Type of Protected Data

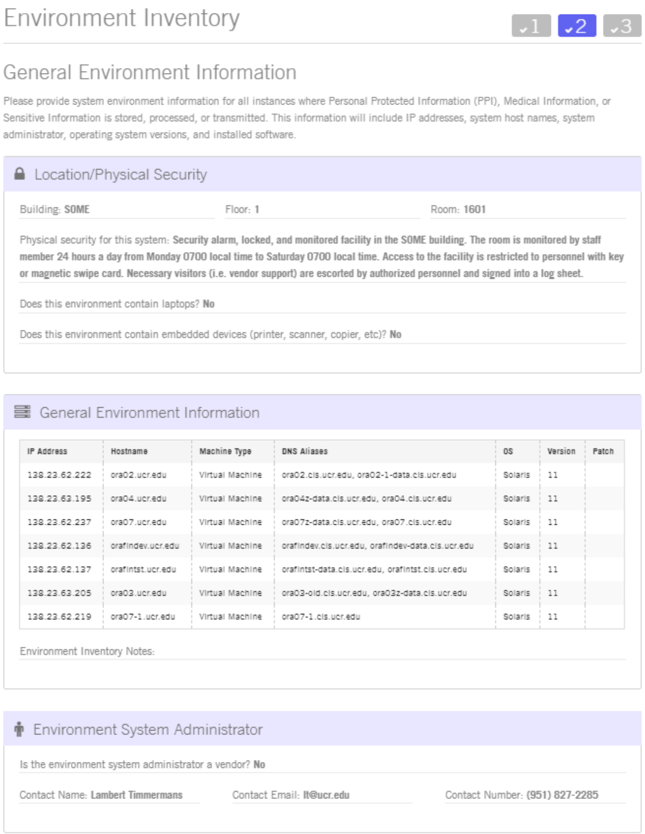
Social Security Number: **No**	Social Security Number Encrypted: **N/A**
Driver's License Number: **No**	Driver's License Number Encrypted: **N/A**
Financial Account or Credit Card Number: **Yes**	Financial Account or Credit Card Number Encrypted: **No**
Medical Information: **No**	Medical Information: **N/A**
Health Insurance Information: **No**	Health Insurance Information Encrypted: **N/A**

Other Sensitive Personal Information

Additional Personal Sensitive Information Keywords: ***None***

Personal Protected Information (PPI), Medical Information, or Sensitive Information contained within environment:

The application guides the user through the process of gathering required information for each system (page 2):



Environment Inventory

General Environment Information

Please provide system environment information for all instances where Personal Protected Information (PPI), Medical Information, or Sensitive Information is stored, processed, or transmitted. This information will include IP addresses, system host names, system administrator, operating system versions, and installed software.

Location/Physical Security

Building: **SOME**

Floor: **1**

Room: **1601**

Physical security for this system: **Security alarm, locked, and monitored facility in the SOME building. The room is monitored by staff member 24 hours a day from Monday 0700 local time to Saturday 0700 local time. Access to the facility is restricted to personnel with key or magnetic swipe card. Necessary visitors (i.e. vendor support) are escorted by authorized personnel and signed into a log sheet.**

Does this environment contain laptops? **No**

Does this environment contain embedded devices (printer, scanner, copier, etc)? **No**

General Environment Information

IP Address	Hostname	Machine Type	DNS Aliases	OS	Version	Patch
138.23.62.222	ora02.ucr.edu	Virtual Machine	ora02.cis.ucr.edu, ora02-1-data.cis.ucr.edu	Solaris	11	
138.23.63.195	ora04.ucr.edu	Virtual Machine	ora04z-data.cis.ucr.edu, ora04.cis.ucr.edu	Solaris	11	
138.23.62.237	ora07.ucr.edu	Virtual Machine	ora07z-data.cis.ucr.edu, ora07.cis.ucr.edu	Solaris	11	
138.23.62.136	orafindev.ucr.edu	Virtual Machine	orafindev.cis.ucr.edu, orafindev-data.cis.ucr.edu	Solaris	11	
138.23.62.137	orafintst.ucr.edu	Virtual Machine	orafintst-data.cis.ucr.edu, orafintst.cis.ucr.edu	Solaris	11	
138.23.63.205	ora03.ucr.edu	Virtual Machine	ora03-old.cis.ucr.edu, ora03z-data.cis.ucr.edu	Solaris	11	
138.23.62.219	ora07-1.ucr.edu	Virtual Machine	ora07-1.cis.ucr.edu	Solaris	11	

Environment Inventory Notes:

Environment System Administrator

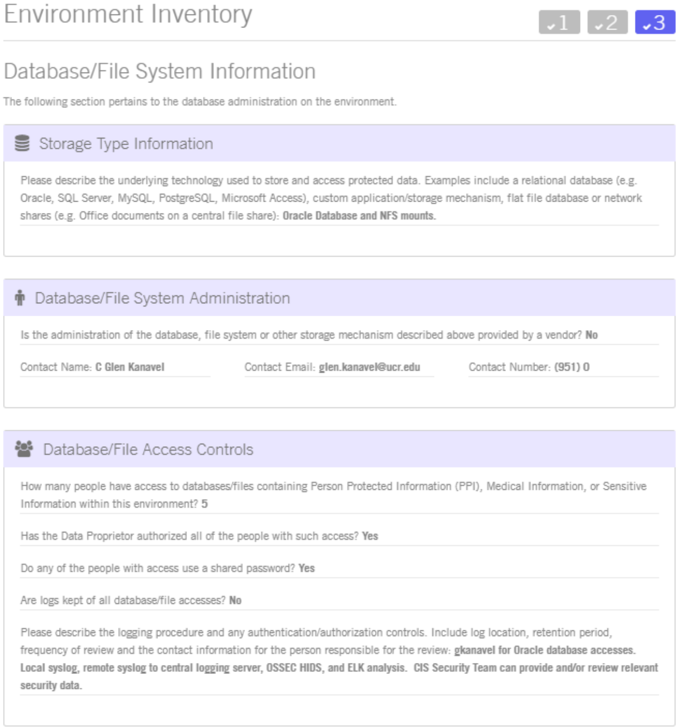
Is the environment system administrator a vendor? **No**

Contact Name: **Lambert Timmermans**

Contact Email: **lt@ucr.edu**

Contact Number: **(951) 827-2285**

The application guides the user through the process of gathering required information for each system (page 3):



Environment Inventory

Database/File System Information

The following section pertains to the database administration on the environment.

Storage Type Information

Please describe the underlying technology used to store and access protected data. Examples include a relational database (e.g. Oracle, SQL Server, MySQL, PostgreSQL, Microsoft Access), custom application/storage mechanism, flat file database or network shares (e.g. Office documents on a central file share): **Oracle Database and NFS mounts.**

Database/File System Administration

Is the administration of the database, file system or other storage mechanism described above provided by a vendor? **No**

Contact Name: **C Glen Kanavel**

Contact Email: **glen.kanavel@ucr.edu**

Contact Number: **(951) 0**

Database/File Access Controls

How many people have access to databases/files containing Person Protected Information (PPI), Medical Information, or Sensitive Information within this environment? **5**

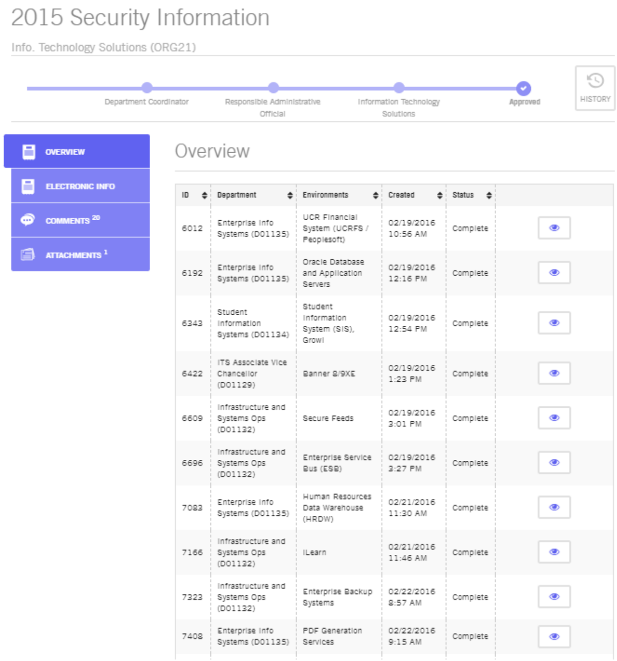
Has the Data Proprietor authorized all of the people with such access? **Yes**

Do any of the people with access use a shared password? **Yes**

Are logs kept of all database/file accesses? **No**

Please describe the logging procedure and any authentication/authorization controls. Include log location, retention period, frequency of review and the contact information for the person responsible for the review: **gkanavel for Oracle database accesses. Local syslog, remote syslog to central logging server, OSSEC HIDS, and ELK analysis. CIS Security Team can provide and/or review relevant security data.**

Overview of systems inventoried within a single IT organization for a specific year (with option to drill-down to view details for each system):



2015 Security Information

Info. Technology Solutions (ORG21)

Overview

ID	Department	Environments	Created	Status	
6012	Enterprise Info Systems (D01135)	UCR Financial System (UCRFS / Peoplesoft)	02/19/2016 10:56 AM	Complete	👁
6192	Enterprise Info Systems (D01135)	Oracle Database and Application Servers	02/19/2016 12:16 PM	Complete	👁
6343	Student Information Systems (D01134)	Student Information System (SIS), Growl	02/19/2016 12:54 PM	Complete	👁
6422	ITS Associate Vice Chancellor (D01129)	Banner 8/9XE	02/19/2016 1:23 PM	Complete	👁
6609	Infrastructure and Systems Ops (D01132)	Secure Feeds	02/19/2016 3:01 PM	Complete	👁
6696	Infrastructure and Systems Ops (D01132)	Enterprise Service Bus (ESB)	02/19/2016 3:27 PM	Complete	👁
7083	Enterprise Info Systems (D01135)	Human Resources Data Warehouse (HRDW)	02/21/2016 11:30 AM	Complete	👁
7166	Infrastructure and Systems Ops (D01132)	iLearn	02/21/2016 11:46 AM	Complete	👁
7323	Infrastructure and Systems Ops (D01132)	Enterprise Backup Systems	02/22/2016 8:57 AM	Complete	👁
7408	Enterprise Info Systems (D01135)	PDF Generation Services	02/22/2016 9:15 AM	Complete	👁