ICPSR | INTER-UNIVERSITY CONSORTIUM FOR POLITICAL AND SOCIAL RESEARCH

A PARTNER IN SOCIAL SCIENCE RESEARCH

# An integrated system for handling restricted use data

Felicia LeClere, Ph.D.

IASSIST 2009

Tampere, Finland

# Data Confidentiality and ICPSR

- Tradition of ICPSR until about 10 years ago was to only handle data that could be put into the public domain
- Substantial change in focus due to changes in data collection methods and the demands of sponsors
- Rethink how we handle confidential data both internally and externally.

# Confidential Data

- Two new initiatives at ICPSR
    - Reorient how we process all data as we do not know which data files may include data the pose disclosure risk
    - Large expansion in restricted use licenses and data that require special dissemination instructions.

# Handling Confidential Data

- Data with identified disclosure risk need to be handled differently
- Need a secure environment in which to clean, process, and store data
- Serves as an processing system for all data in the future

# Secure Processing Initiative

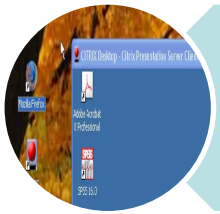
- Technical Requirements
- Solution for Windows Environment

# Technical Requirements

- Network isolation
- Operating system and application isolation
- Separate data storage
- Accessible on-site or remotely through VPN
- Processing tools for *nix and Windows environments
- Seamless integration with existing workflow

# Windows Environment


Agent



Desktop


Web

- Three ways to access Citrix
- Applications are isolated
- Familiar Windows look and feel

# Citrix Agent

Access provided through

- Start Menu


- Desktop Icon

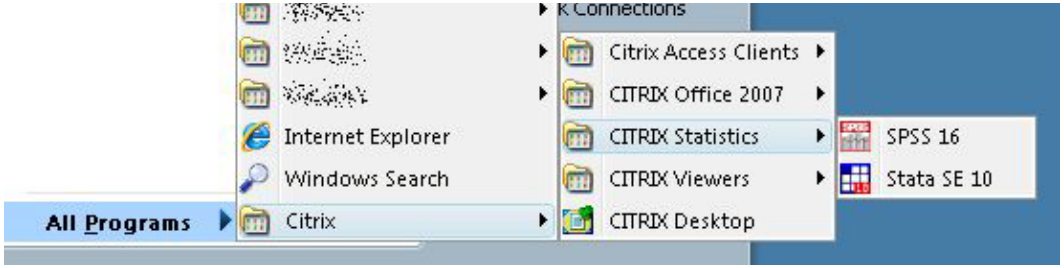
# Citrix Program Neighborhood Agent

Applications can be accessed from system tray


Applications cannot access any files on host system

Citrix application folders also added to Start menu

Folders available while Agent active



# Citrix Desktop Client

- Self-contained environment
- Runs in a separate window
- Isolated from host computer
- Familiar look and feel

# Automating restricted use contracting

- Current practice is a paper based with all documents from the contract held in paper
- Data are transmitted through encrypted CD
- Administrators monitor contracts through ACCESS, Excel, or some other method
- Very time consuming for data systems with a large number of contract holders

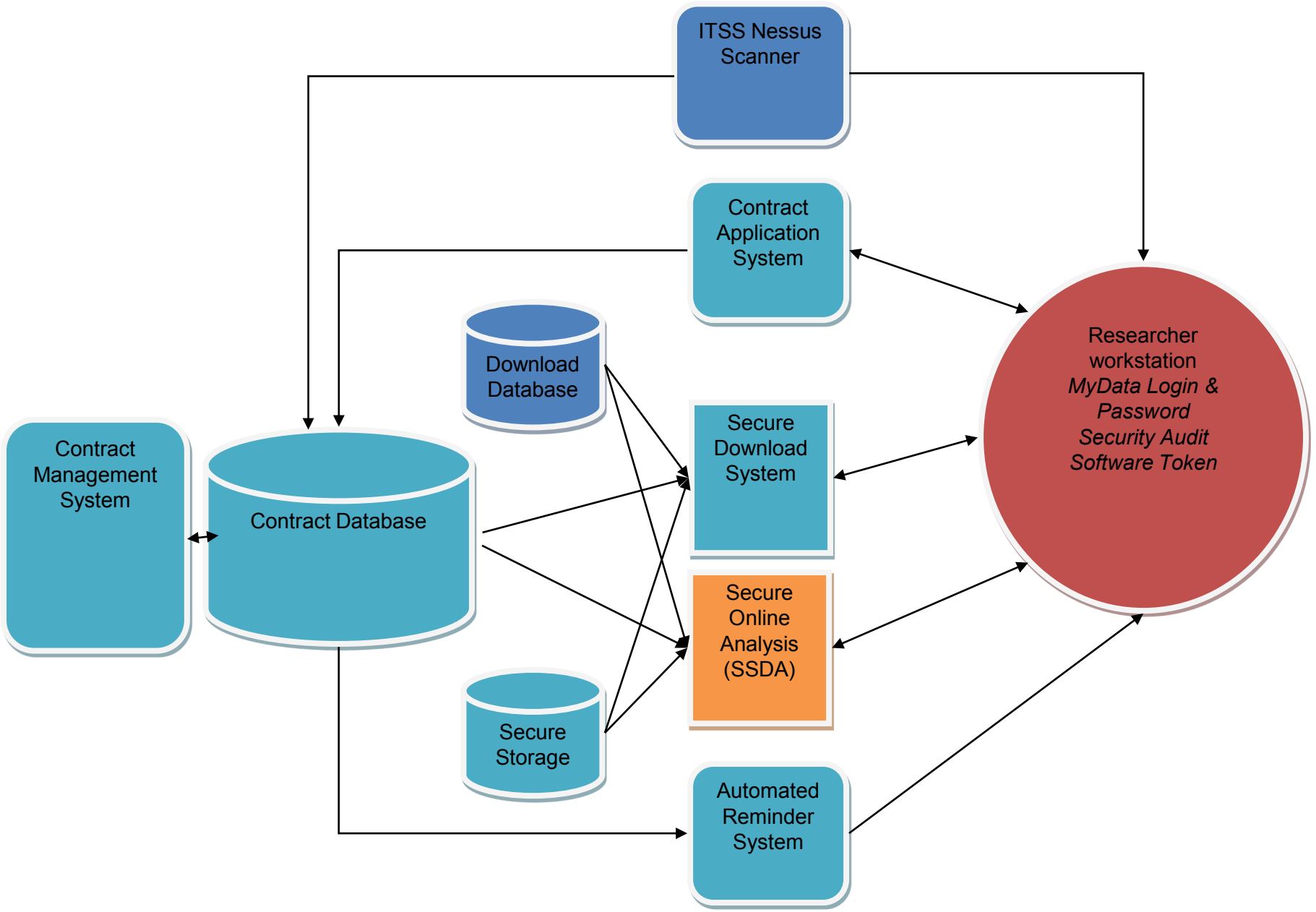
# Innovations in the RCS

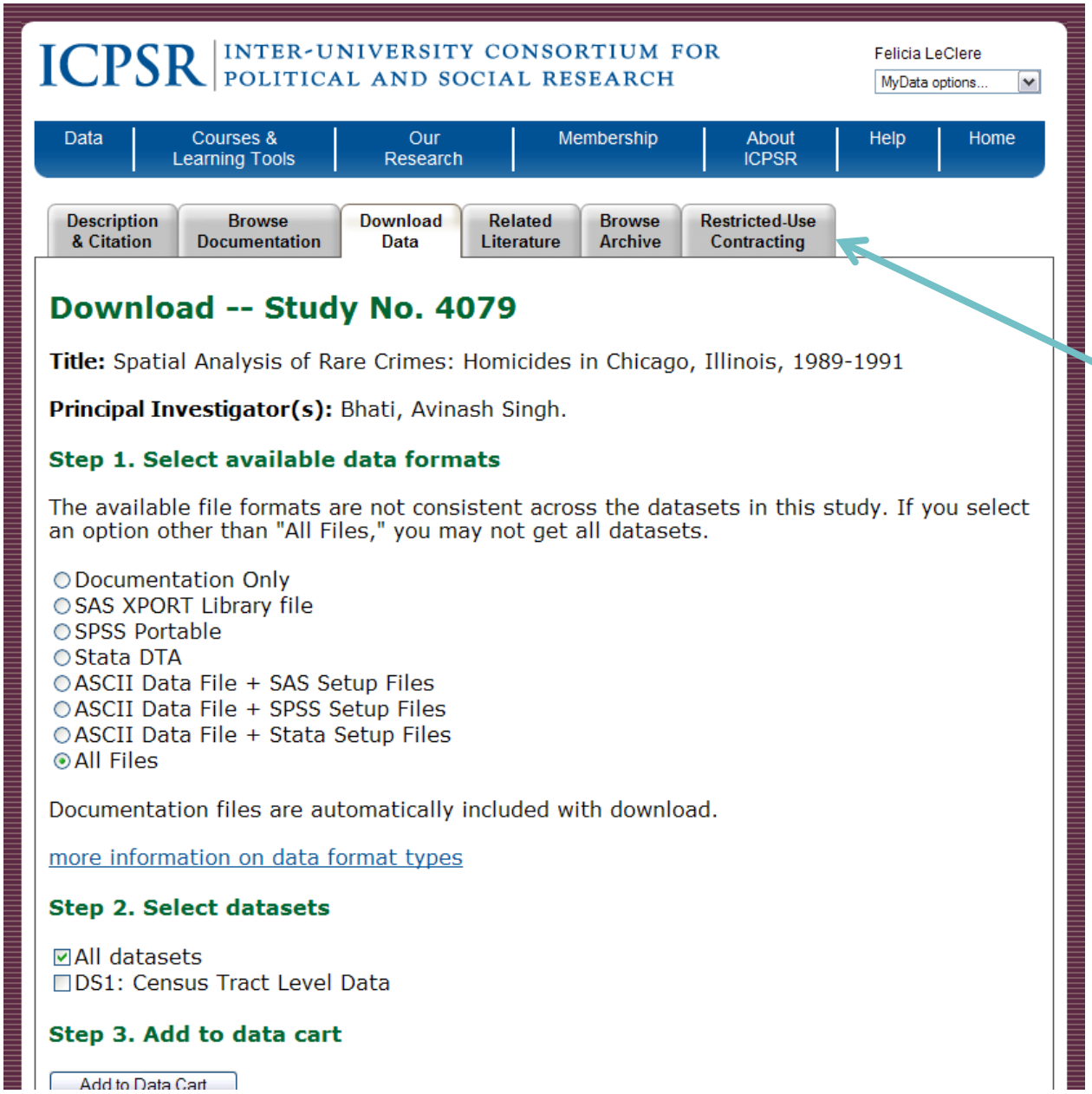
- All electronic signatures except institutional representatives

- Changes in security evaluation
    - Behavioral checklist
    - Network scan conducted by ITSS, Michigan
    - Freeware workstation audits

# Innovations in the RCS

- Secure download of data
  - 2-factor authentication
  - Triggered by contract approval
  - Single download with manual override


ITSS Nessus Scanner
Contract Application System
Researcher workstation
MyData Login &
Password
Security Audit
Software Token
Download Database
Contract Management System
Contract Database
Secure Download System
Secure Online Analysis (SSDA)
Secure Storage
Automated Reminder System



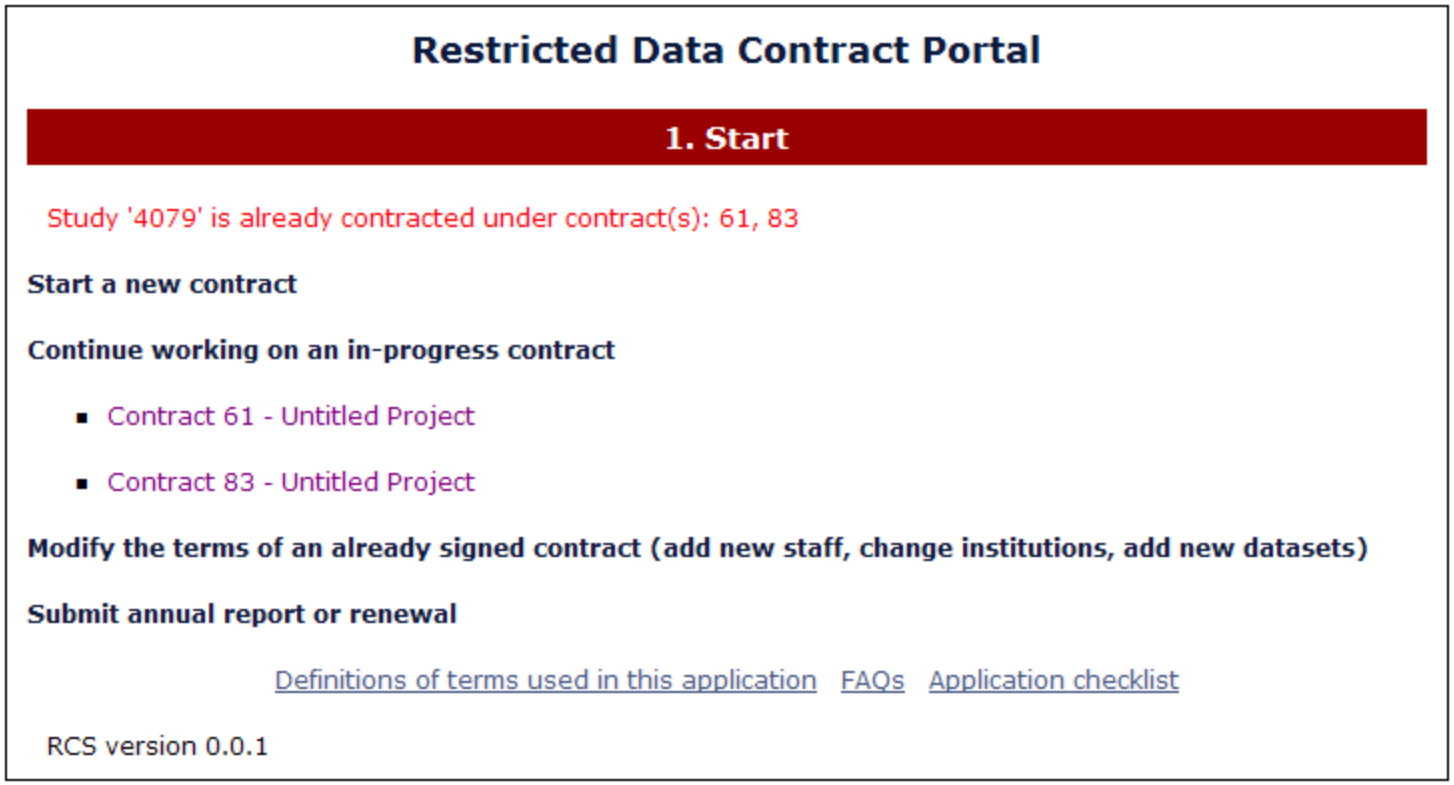

Method of Access to Contracting System

# Application flow

- Based on ICPSR's authentication system *MYDATA* for the applicant

- Allows for return to upload additional components
    - IRB approval
    - Scanned signature pages
    - Revised contract terms

# USER INTERFACE



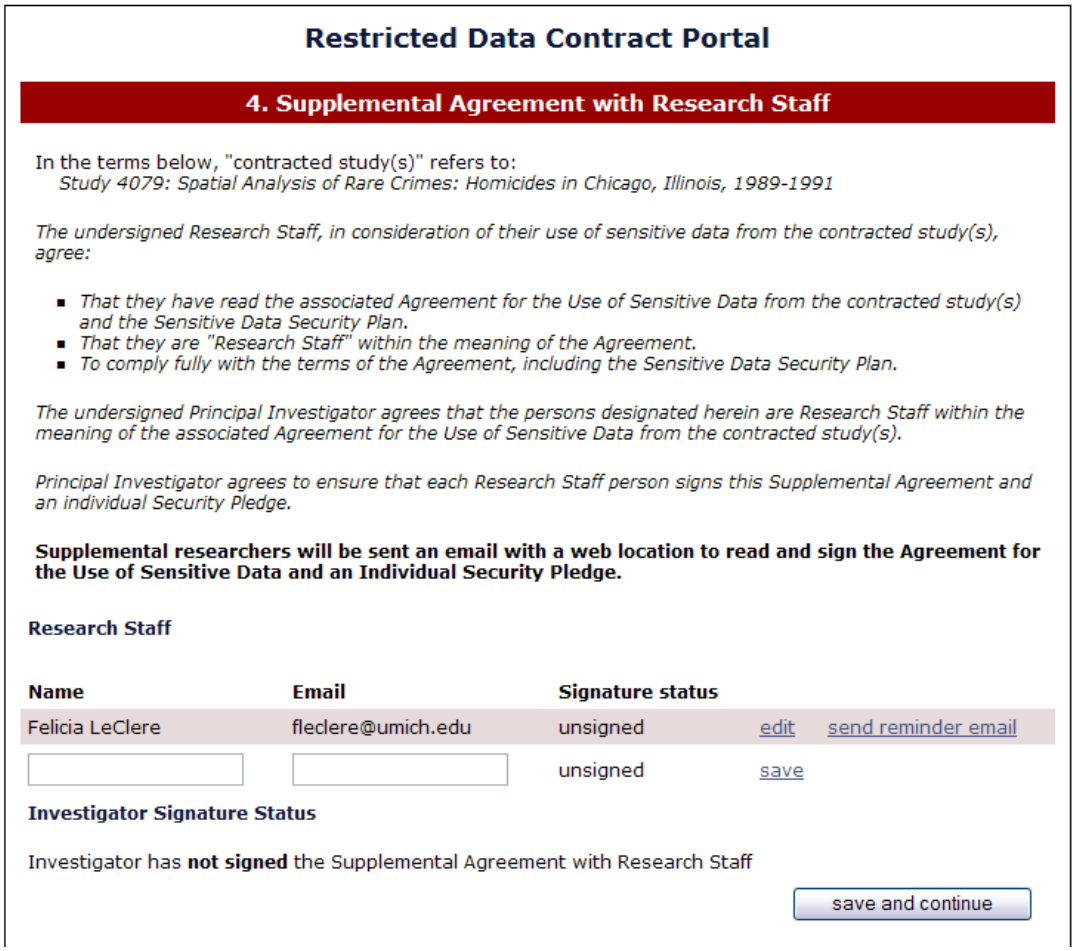
# Signature Process

## Two approaches

-for primary investigator and research staff, we will accept electronic signature. Each will be sent an email that directs them to a signature page.

- for institutional representative, the p.i. will be sent an email with a signature page that will need to be signed, scanned, and uploaded.

# Signature for researchers



**Restricted Data Contract Portal**

**4. Supplemental Agreement with Research Staff**

In the terms below, "contracted study(s)" refers to:
*Study 4079: Spatial Analysis of Rare Crimes: Homicides in Chicago, Illinois, 1989-1991*

*The undersigned Research Staff, in consideration of their use of sensitive data from the contracted study(s), agree:*

- *That they have read the associated Agreement for the Use of Sensitive Data from the contracted study(s) and the Sensitive Data Security Plan.*
- *That they are "Research Staff" within the meaning of the Agreement.*
- *To comply fully with the terms of the Agreement, including the Sensitive Data Security Plan.*

*The undersigned Principal Investigator agrees that the persons designated herein are Research Staff within the meaning of the associated Agreement for the Use of Sensitive Data from the contracted study(s).*

*Principal Investigator agrees to ensure that each Research Staff person signs this Supplemental Agreement and an individual Security Pledge.*

**Supplemental researchers will be sent an email with a web location to read and sign the Agreement for the Use of Sensitive Data and an Individual Security Pledge.**

**Research Staff**

| Name | Email | Signature status | | |
|---|---|---|---|---|
| Felicia LeClere | fleclere@umich.edu | unsigned | edit | send reminder email |
| | | unsigned | save | |

**Investigator Signature Status**

Investigator has **not signed** the Supplemental Agreement with Research Staff

save and continue

Add researchers and send email for signature

# Researchers' email signature page

**Restricted Data Contract Portal**

**Electronic Signatures**

**Contract 83 - Untitled Project**

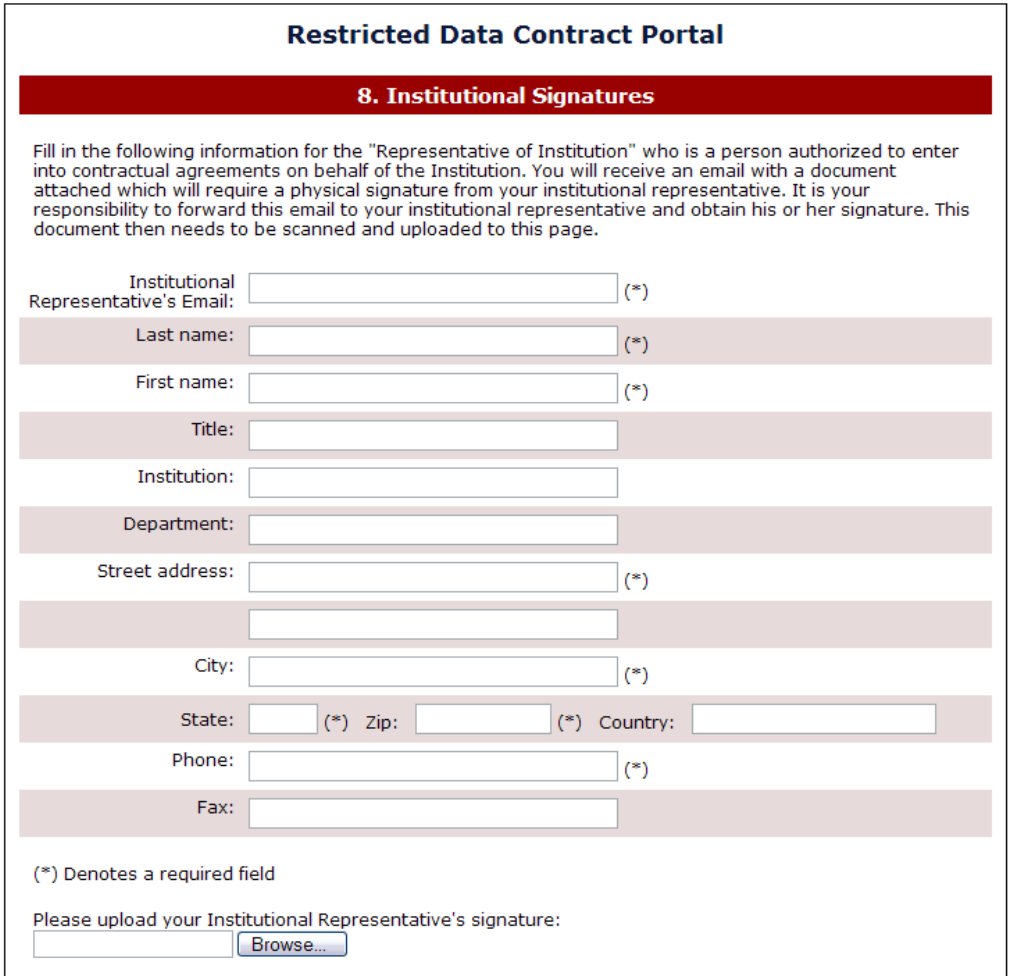
**Studies under contract:**
*Study 4079: Spatial Analysis of Rare Crimes: Homicides in Chicago, Illinois, 1989-1991*

In order to provide your electronic signature, click the link that says "sign here."

| name | role | signature status | file |
|---|---|---|---|
| Felicia LeClere | Researcher | sign here | agreement terms (PDF 22K) |

Lists all of the researchers, provides agreement terms, and a clickable signature field

# Institutional representatives signature



**Restricted Data Contract Portal**

**8. Institutional Signatures**

Fill in the following information for the "Representative of Institution" who is a person authorized to enter into contractual agreements on behalf of the Institution. You will receive an email with a document attached which will require a physical signature from your institutional representative. It is your responsibility to forward this email to your institutional representative and obtain his or her signature. This document then needs to be scanned and uploaded to this page.

Institutional Representative's Email: (*)
Last name: (*)
First name: (*)
Title:
Institution:
Department:
Street address: (*)
City: (*)
State: (*) Zip: (*) Country:
Phone: (*)
Fax:

(*) Denotes a required field

Please upload your Institutional Representative's signature:
Browse...

There will be a document attached to the email to be sent to PI that will be signed by Institutional Representative.

# Security orientation

Current orientation is a “trust me” orientation with very high burden for users to assess computer security

New orientation ---provide users with tools to assess security

# Security Process

- Three components
  - Behavioral components
  - Network Security
  - Workstation security

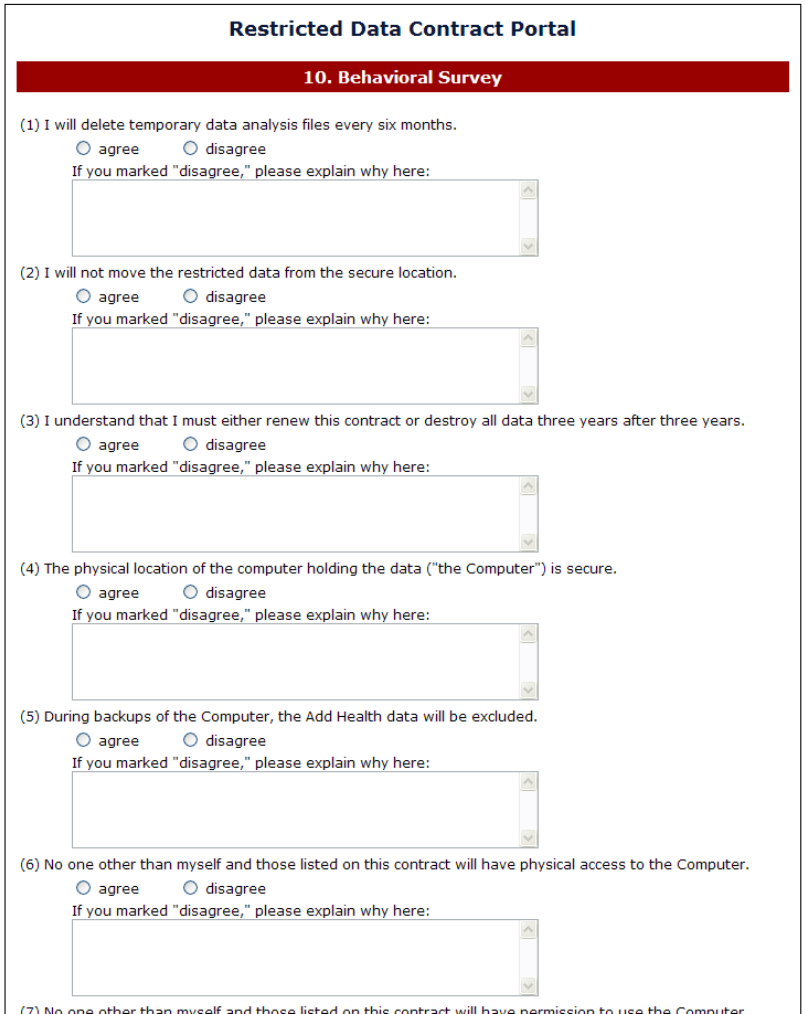
# How we approach security

- Two security focuses

  Where the data are stored

  Where users will be analyzing the data

# Behavioral questions



**Restricted Data Contract Portal**

**10. Behavioral Survey**

(1) I will delete temporary data analysis files every six months.
agree disagree
If you marked "disagree," please explain why here:

(2) I will not move the restricted data from the secure location.
agree disagree
If you marked "disagree," please explain why here:

(3) I understand that I must either renew this contract or destroy all data three years after three years.
agree disagree
If you marked "disagree," please explain why here:

(4) The physical location of the computer holding the data ("the Computer") is secure.
agree disagree
If you marked "disagree," please explain why here:

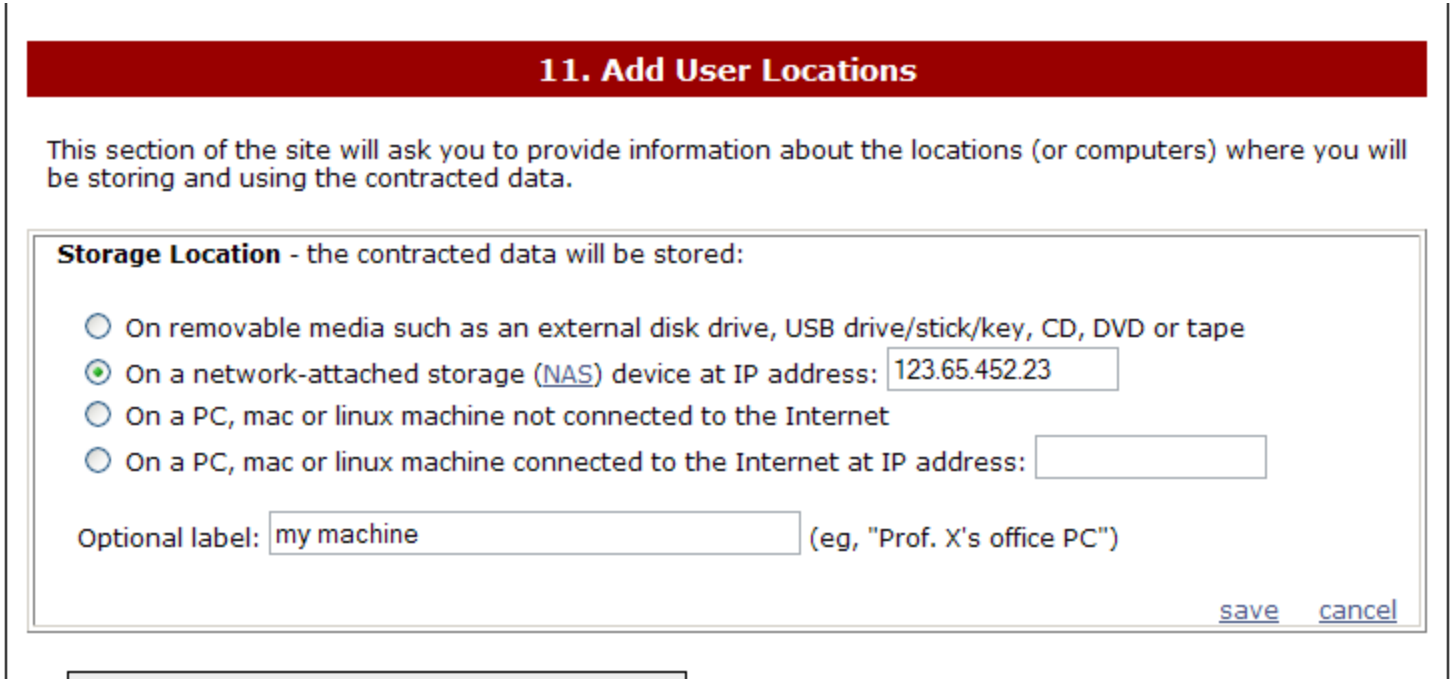
(5) During backups of the Computer, the Add Health data will be excluded.
agree disagree
If you marked "disagree," please explain why here:

(6) No one other than myself and those listed on this contract will have physical access to the Computer.
agree disagree
If you marked "disagree," please explain why here:

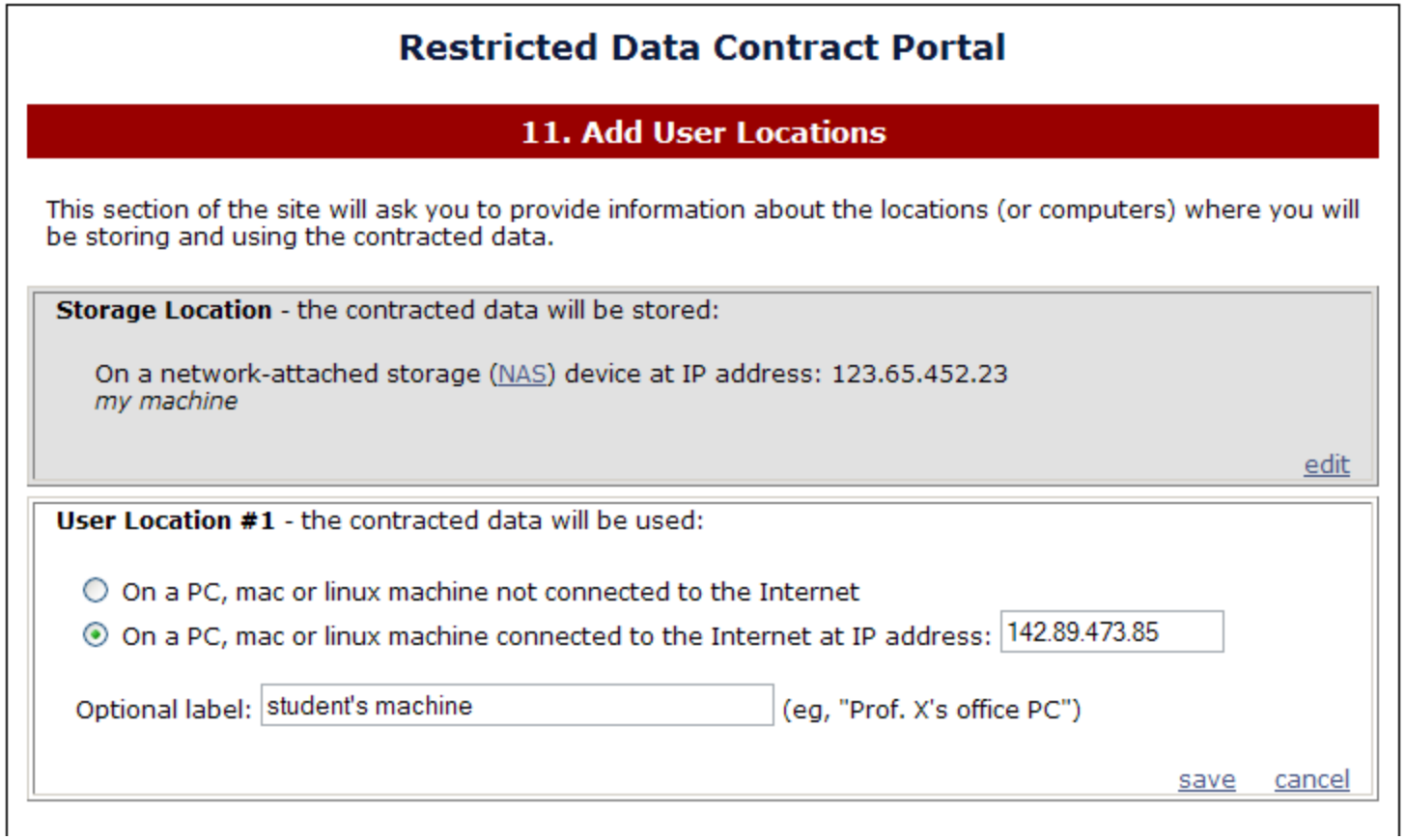
(7) No one other than myself and those listed on this contract will have permission to use the Computer

Allows users to justify some departures from appropriate secure data behaviors.

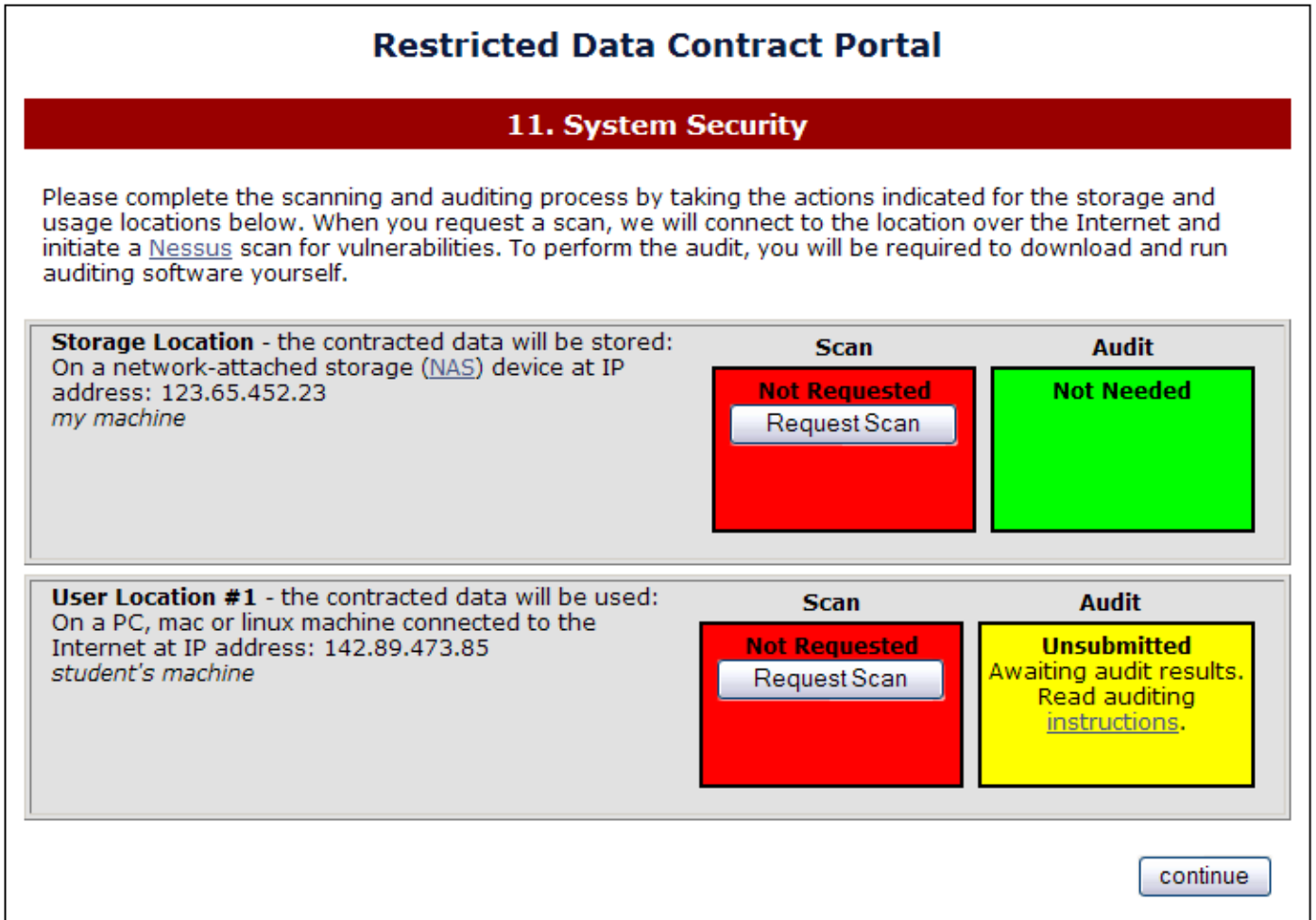
# Setting up *storage* location



# Setting up *user* locations



# Using the security dashboard



# What this tells us

The NAS storage device and the workstation will need a SCAN (which is a NESSUS scan conducted by ITSS at the University of Michigan). The button request will run it and generate results that our staff will evaluate.

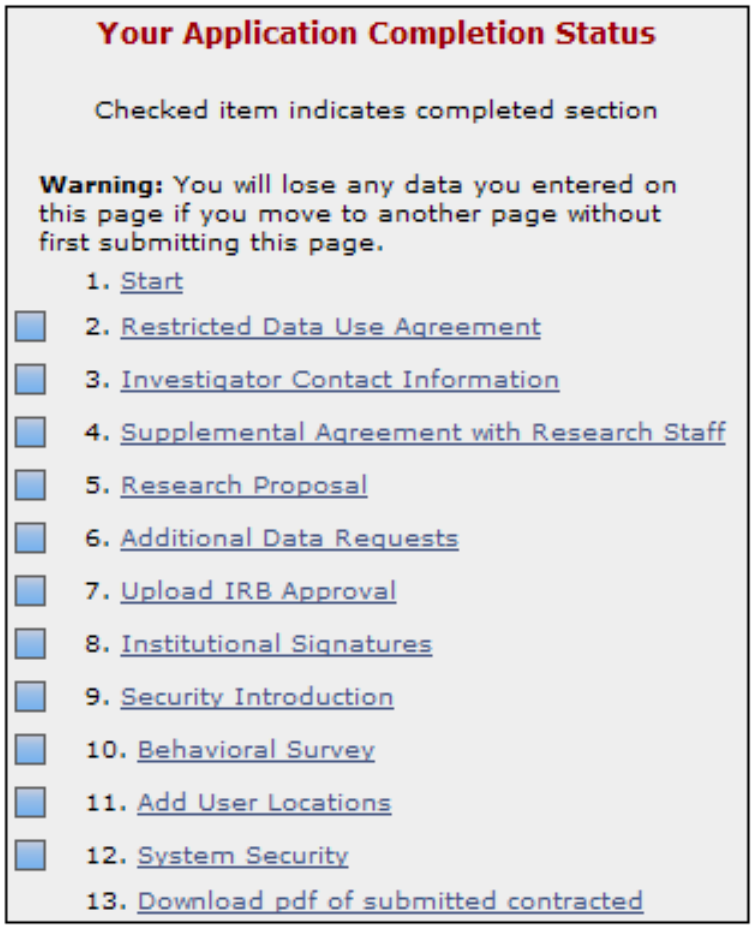
If the block turns green, the system passes. If it is yellow, it means that you will need to retrieve response, remedy security issues, and rescan.

# What this tells us

The Audit is only required for the workstation.

The clickable instructions will provide the users with instructions about how to download freeware and run it.

The results of the audit will be emailed to our staff. The block again will turn green if no changes are necessary. The block will be red and a clickable link will provide users with instructions on how to resolve security issues




Navigation panel for user interface

# Backend system

- Administrative portal
- Reporting System
- Automated email system to send reminders
- Secure Download System

# Display a Contract

**Contract Number:** 1
**Contact:** Jon Brode
( brode@icpsr.umich.edu )
**PI:** Felicia LeClere
**Archive:** HMCA
**Study(s):** 4079, 4232
**Assignee:** brode change
**Status:** Under Review; Initial change
**Survey Status:** Under Review change review answers
**Expires:** 01-JAN-10 change
**Institutional Signature:** Uploaded on 16-APR-09 13:08
download change
**Notarized Affidavit:** Uploaded on 24-APR-09 14:38
download change
**Modified Contract:** Uploaded on 11-MAY-09 17:40
download change
**Notes:**
These are the notes.

change

---

## Security Detail

| Host | Scan | Audit |
|---|---|---|
| **Storage Location (1)**<br>removable media<br>"Jon's USB stick" | **Not Needed** | **Not Needed** |
| **Usage Location (2)**<br>internet pc<br>141.211.192.30 | **Scan Pending** | **Failed** |

# Restricted Data Contract Portal
# Administrative Interface

| Contract Status | Owner | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | CCEERC | DATAPASS | DSDR | HMCA | ICPSR | MDRC | NACDA | NACJD | SAMHDA | ALL |
| Under Review; Initial | | | | | 4 | | | 4 | | 8 |
| Active; Original | | | | | | | | | | |
| Under Review; Renewal | | | | | | | | | | |
| Active; Renewal | | | | | | | | | | |
| Expired; Affidavit | | | | | | | | | | |
| Expired; No Affidavit | | | | | | | | | | |
| Expired; Limbo | | | | | | | | | | |
| Denied | | | | | | | | | | |
| Total | | | | | 4 | | | 4 | | 8 |

# Restricted Data Contract Portal
# Administrative Interface

**ICPSR Contracts (4)**

| Status | Contract Number | PI | Project title | ICPSR study # | Date contract complete | Date of renewal | Date of expiration | IRB expiration date | Assigned to | Files downloaded? | 2-month reminder sent? | 1-month reminder sent? |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Under Review; Initial (4)** | 1 | Felicia LeClere | Taming of the Shrew | 4079 4232 | 19-MAR-09 | | 01-JAN-10 | 01-JAN-11 | brode | No | | |
| | 63 | mary morris | No Title | 4232 | | | | | | No | | |
| | 21 | Lisa Neidert | No Title | 4079 4232 | | | | 02-MAR-10 | | No | | |
| | 101 | | No Title | 4079 4232 | | | | | | No | | |

# Future

- Roll out with the Panel Study of Income Dynamics in September 2009 and the National Longitudinal Study of Adolescent Health in January 2010.

- Proposal into NIH to move data storage and analysis to the “computing cloud” -- that is utility computing on the internet.