



You want me to do what?  
Musings on writing a System Security Plan with labs.

Mike Warfe

Assistant Director Research Computing



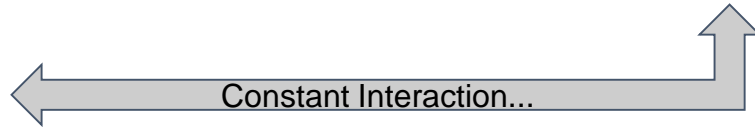
# Goals of my talk

- Overview of my organization and the role we play
- Tell a story (the musing part)
- Provide an overview of a Systems Security Plan
- Provide some tips that I have found impactful
- Answer questions if time permits



# UTech Research Services and Resources Overview

- Research Computing Services
  - HPC (Basic Research)
  - Storage (Basic Research)
  - Virtualization
    - Secure Research Environment (Restricted Research)
    - Research VMs (Basic Research)
  - Applications
- Research Computing Staff
  - Service Managers
  - CI Engineers
  - Technologists (Engineering, Medical, Humanities, Hard Sciences, **Compliance**)
- Information Security
  - Policy Makers
  - Incident Handlers



# UTech Research Computing Role

- Run Services
  - Onboard Users to service through activation and provide training.
  - Provide Support through Email, Help Desk, Phone Calls, Office Visits...
  - Maintain service strategy, operations, and life cycle of service.
- Optimize Services for Users
  - Provide solutions instead of services
  - Partner with labs on opportunities (pre-award, award, publication)
  - Governance activities
- Influence Policy and Strategy for supporting Research
  - Central IT and Information Security
  - Research Administration
    - Institutional Review Board
  - Schools and Colleges
  - General Counsel



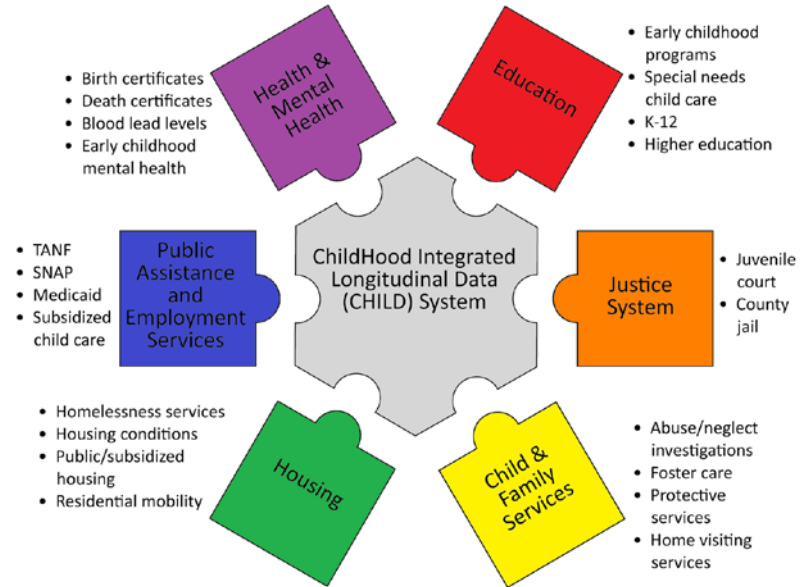
# CHILD System

The system is nationally recognized as among the oldest and most comprehensive in the country and includes continually updated administrative data from **1989** to the present from 35 administrative systems on more than **640,000 children**, for a total of nearly 200 million records in the system.

Funding for CHILD comes via grants from Cuyahoga County, the MacArthur Foundation, the City of Cleveland, and others.

The CHILD system is used by Poverty Center researchers for research and evaluation of over a dozen projects.

PIs: Claudia Coulton, Ph.D and Rob Fischer, Ph.D



Source: <http://povertycenter.case.edu/data-systems/child-data-system/>

# Onboarding Poverty Center into the SRE

- Assessment of Needs
  - Contract Review
  - Privacy Impact Assessment
  - IRB Protocol Review
  - Solution Architecture
    - Usage of RDS Host instead of VMWare View Desktop
    - Application Inventory
- Assignment of Tenant Coordinator
- Training of Users
- Collaboration on SSP, DMP, Future proposals

# Example System Security Plan

1. Information System Name / Title
2. Information System Categorization
  - a. Low
  - b. Moderate
  - c. High
3. Information System Owner
4. Authorizing Official
5. Other Designated Contacts
6. Assignment of Security Responsibility
7. Information System Operational Status
  - a. Test
  - b. Dev
  - c. Prod
8. Information System Type
  - a. Major Application
  - b. General Support System
9. General System Description / Purpose
10. System Environment
11. System Interconnections / Information Sharing
  - a. Name, Org, Type (MOU,MTA,DUA), Agreement, Date, FIPS Category, C&A Status, Auth Official
12. Related Laws / Regulations / Policies
13. Risk Assessment
  - a. Major
  - b. Minor
14. Minimum Security Controls
  - a. CUI
  - b. FISMA
  - c. HIPAA
15. Information Security Plan Completion Date
16. Information Security Plan Approval Date



# Tips for Success

1. Build **relationships** that are not transactional
  - Listen and show empathy
  - Invest time and build influence
2. You are **presenting** change to the lab
  - 5 P's (in presenting change) Purpose - Picture - Plan - Part - Practice
3. Rome wasn't built in a day
  - **Important work takes time**
  - **Small incremental changes** and continued progress **are easier to achieve** than alternatives  
(Sit on your hands or Blow everything up)
4. **Security plans** should be treated as **living documents**
  - Both Tech and Labs change over time
  - Identify all risks, but be flexible and *mitigate the risks you cannot tolerate.*





# Questions and Thanks