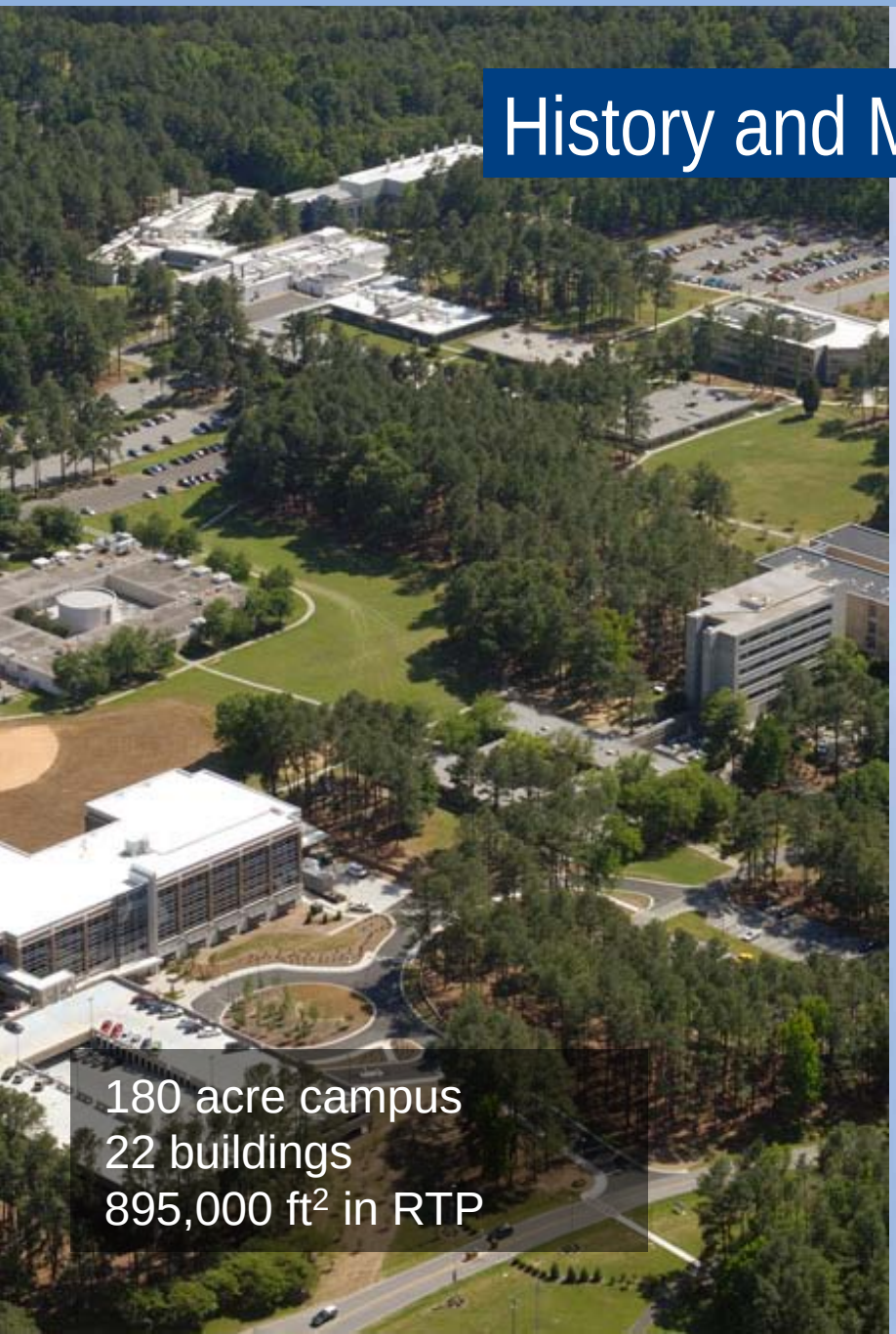
Working in a FIPS Moderate Environment at RTI International

Information Technology and Infrastructure

FedCASIC

March 23, 2011

History and Mission



- Independent, not-for-profit research and development organization
- Founded in 1958 through a partnership between business leaders, state government, and area universities
- Mission: to improve the human condition by turning knowledge into practice
- One of the world's leading research institutes

Office Locations

Headquartered in North Carolina, with satellite and project offices around the world

Research Triangle Park, NC

Washington, DC

Rockville, MD

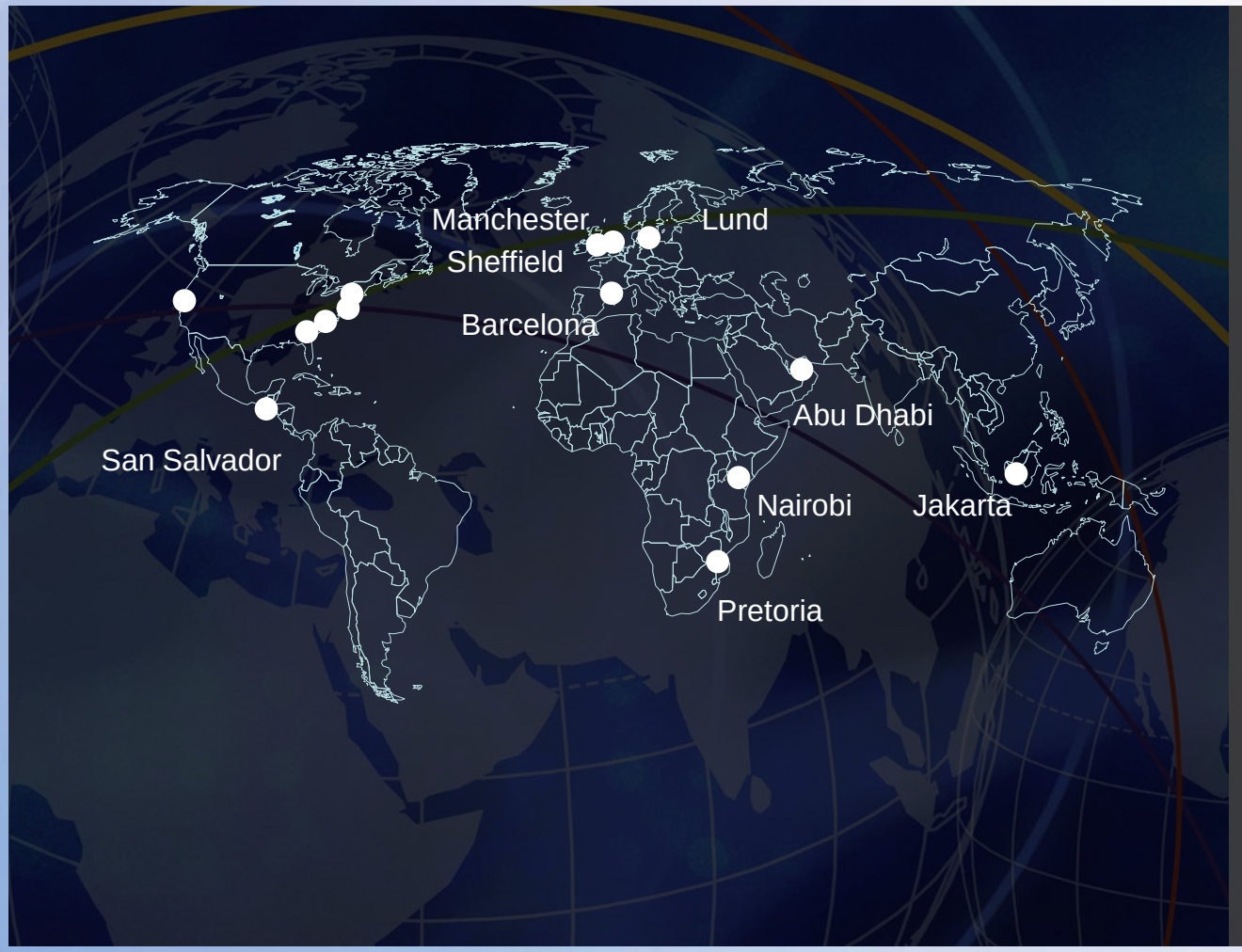
Atlanta, GA

Chicago, IL

Waltham, MA

San Francisco, CA

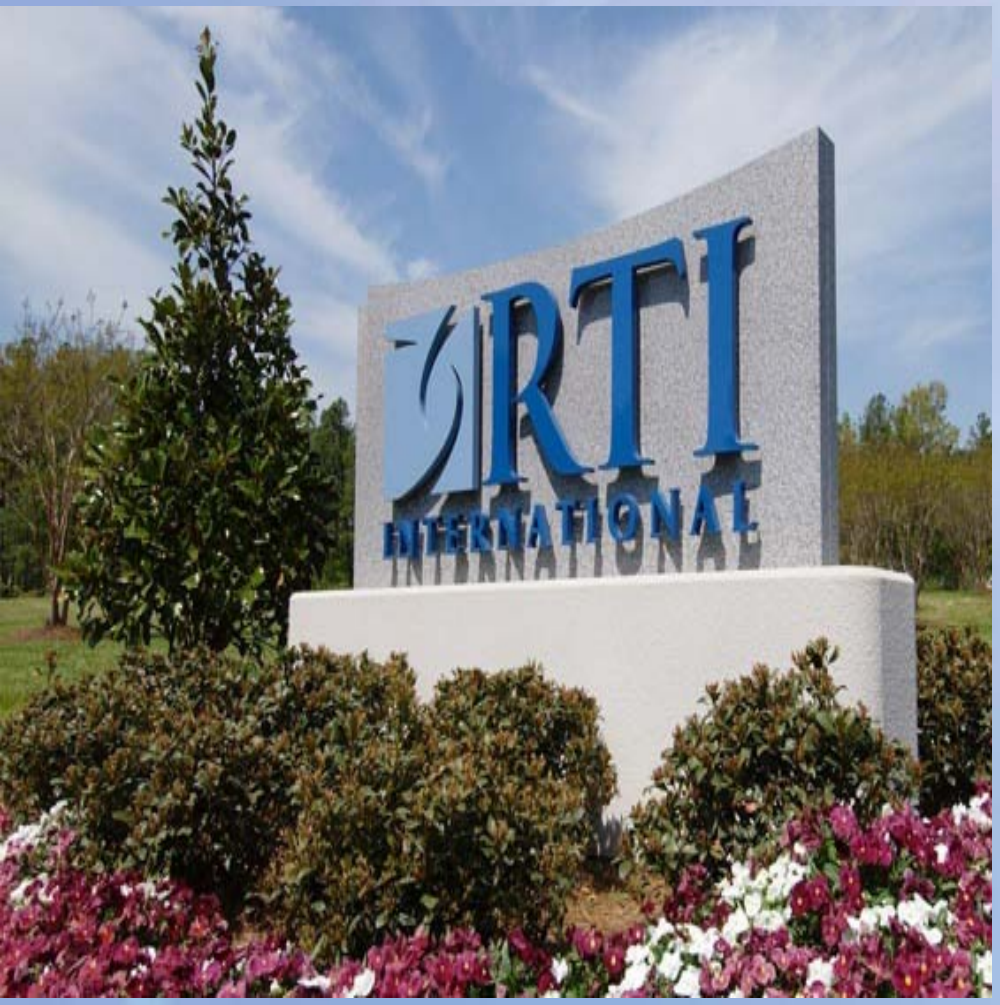
Ann Arbor, MI



Our People

- 2,300 in North Carolina
- 500 in U.S. regional offices
- 1,200 supporting international development projects
- More than 130 disciplines
  - Statistics
  - Survey methodology
  - Public health
  - Epidemiology
  - Economics
  - Chemistry and life sciences
  - Engineering

Data Security at RTI International



- Extensive Application Development and Data Collection on behalf of Federal Agencies and Commercial Clients
- Multiple Certified & Accredited General Support Systems and Major Applications handling Low and Moderate Risk Data

Institute Level Data Security

Implementing a FIPS Moderate Environment

Jennifer Durbin
Information Security Officer

Federal Regulation Compliance

- FISMA *Federal Information Security Management Act of 2002*
- The Privacy Act of 1974
- CIPSEA *Confidential Information Protection and Statistical Efficiency Act of 2002*
- HIPAA *Health Insurance Portability and Accountability Act of 1996*
- HITECH Act *Health Information Technology for Economic and Clinical Care Act of 2009*
- GINA *Genetic Information Nondiscrimination Act of 2008*
- OMB A-130 Management of Federal Information Resources
- International Data Privacy Laws

Data Security Compliance Implementation

- Enhanced Security Network (ESN)
  - A Moderate Security Network physically and logically separate from the other RTI networks with NO direct/local connection (via network port, etc.)
- IT Security & Compliance
  - Information Security Program Management
    - Senior Information Security Officer
    - Security Control Assessors
- Information Security Officer
- Privacy Officer (IRB)
- Internal Partnerships
  - Business Units, Project Directors, Application Developers

Data Security Policies and Training

- Data Handling Guidelines (PII, PHI, Sensitive, etc.)
  - Proper use
  - Required protections
- IT Security Awareness Training
  - Required for all new employees and annually thereafter
  - Topics covered
    - Data Privacy
    - Email Security
    - Laptop Security
    - Protecting Confidential Information
- Project Specific Data Security Training
- Regular Data Security Communications

Security Control Implementation

- Numerous Authorized General Support Systems and Major Applications
  - Designed/re-designed to meet all Security Objectives based upon the Potential Impact
    - Security Objectives
      - Confidentiality
      - Integrity
      - Availability
    - Potential Impact
      - Low
      - Moderate
      - High
  - NIST SP 800-37 Rev. 1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
    - NIST SP 800-53 Rev. 3: Recommended Security Controls for Federal Information Systems and Organizations
- Interconnection Security Agreements

Key Moderate Risk Security Controls

- Access to data within the Enhanced Security Network (ESN) requires 2-factor authentication
  - Something you know = PIN
  - Something you have = token
- Data moved outside of the ESN must be appropriately encrypted (FIPS 140-2)
- E-mail use is restricted (outbound only, limited size, no attachments)
- All printing must be encrypted
- Extremely limited internet access from within the ESN
  - Default deny

Key Moderate Risk Security Controls (cont.)

- Physical Security Controls
  - Restricted access
  - Fire suppression
  - Climate controls
  - Uninterruptible power supplies
  - Cameras on access doors
  - Visitor escorts
  - Visitor sign-in / sign-out
    - Sign Confidentiality Agreements (where applicable)
  - Periodic inspections by security staff
  - Periodic audits of data center and visitor logs

Key Ongoing/Other Data Security Measures

- Continuous Monitoring Program
  - Vulnerability Scanning
  - Penetration Testing
- Periodic and Unannounced Audits
- Regular Agency testing
- Continuous Process Improvement (ITIL)
- PoAM Tracking
- Information Security Incident Reporting and Tracking
- Document Management
- Federal Regulation and Best Practices Monitoring

RTI-CCS Data Security Implications

Data Collection Facility

McKinlay Jeannis

Call Center Services, Project Supervisor

RTI-CCS' scope of ensuring data security

- Operates 7 days a week and 8-14 hours per day
- 17,000 square feet
- 240 production stations
- 600 staff when operating at maximum capacity (both RTI and temporary staff)

Data Security within RTI-CCS

- RTI aggressively navigated the implementation for access to the enhanced security network (ESN) to ensure that all projects containing personal identifying information and personal health information are FIPS moderate compliant as of 2008.

- Our data collection systems has been modified to operate in either a FIPS Low or Moderate environment
  - The strength of our existing operational controls enabled us to more easily comply with the rigorous data security requirement for a Moderate environment

Operational Security Controls

- Facility Security
  - Enhanced CCS Security Measures
    - Door Code
    - Visitor Confidentiality Agreement Form
    - Electronic devices are required to be powered off

- Hiring and Training process
  - Screening
    - nationwide 7 year criminal background check
    - credit checks (when applicable)
  - Training
    - System and network access granted only upon successful completion of General Training
    - Initial and ongoing trainings addressing data security and privacy

Operational Security Controls (cont.)

- Account Creation and Project Assignment Process

  Electronic Request and Approval
  - RTI-CCS proprietary tracking application
  - Provides an audit trail for account creation
  - Includes the activation and deactivation of staff

  Hierarchal Structure of Approval
  - Approval granted by authority level above submitter

Operational Security Controls (cont.)

- Log in Credentials and Passwords
  - Log in
    - Unique User names assigned to every employee
  - Passwords
    - Multiple layers of password requirements
      - Domain and network access
      - ESN
    - Systems enforce complex password requirements
      - Complex password requirements are defined as;
        - Minimum length and complexity
        - Passwords changed frequently
        - Previously used passwords cannot be reused
    - Two Factor Authentication

Operational Challenges with Data Security

- Costly and Labor Intensive Set Up
  - Networks and systems are logically segregated requiring the creation of multiple accounts
  - Tokens required for 2-factor authentication must be logically and physically managed
- Managing Accounts
  - Reset of Passwords
- Multiple layers of security screening
  - Various project requirements

Contact Information

Jennifer Durbin
Information Security Officer
919.316.3362
jenni@rti.org

Tamara Terry
Research Services Manager
919.926.6560
tterry@rti.org

McKinlay Jeannis
CCS Project Supervisor
919.926.6519
mjeannis@rti.org

David Foster
Manager, Applications & Systems Analysis
919.926.6510
dfoster@rti.org