Implementing a FIPS-Moderate Security Model on a Large Household Survey

Pete Tice, Karen Davis, Tennyson Chen, Becky Granger, Fred Huebner,
R. Suresh, Hilary Zelko, Martin Meyer

Acknowledgements

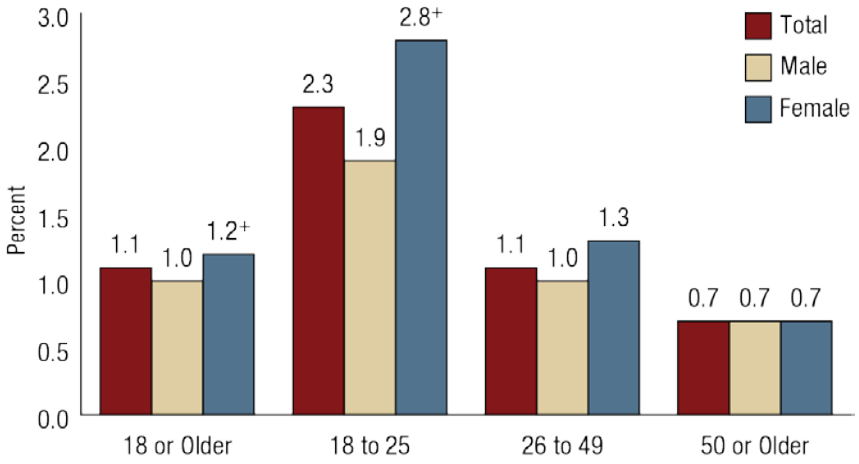
- The presentation stems from ongoing work conducted under the contract for the National Survey on Drug Use and Health (NSDUH). The NSDUH is funded by the Substance Abuse and Mental Health Services Administration (SAMHSA), Center for Behavioral Health Statistics and Quality under contract no. 283-2013-00001C and project no. 0213986 and 0213985.
- The views expressed in this presentation do not necessarily reflect the official position or policies of SAMHSA or the U.S. Department of Health and Human Services; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

National Survey on Drug Use and Health (NSDUH)

- The NSDUH is an annual household survey that provides national, state and substate level estimates on the use of tobacco products, alcohol, illegal drugs and on mental health in the civilian, noninstitutionalized population age 12 and older.
- RTI supplies a robust IT infrastructure that supports approx. 1,200 users. Software development, IT infrastructure, help desk, logistics.
- Several project web sites, fleet of 2,500 laptop and tablets for in-field data collection.

NSDUH

NATIONAL SURVEY ON DRUG USE AND HEALTH



NSDUH Requirements

- Four active NSDUH surveys in various stages of completion:
  1. Pre-data collection survey preparation (e.g., 2018 NSDUH)
  2. Data collection (e.g., 2017 NSDUH)
  3. Post data collection data processing, analysis/reporting, and data file preparation (e.g., 2016 NSDUH)
  4. Continued analysis/reporting and final survey documentation (e.g., 2015 NSDUH)

- Quarterly data collection each year
  - 600 field interviewers
  - Across all 50 states and the District of Columbia
  - 140,000 household screenings
  - 67,500 interviews completed annually

- Support SAMHSA releasing First Findings Reports and Detailed Tables within 9 months post data collection

- Creation of public-use data files for dissemination within 11-12 months post data collection

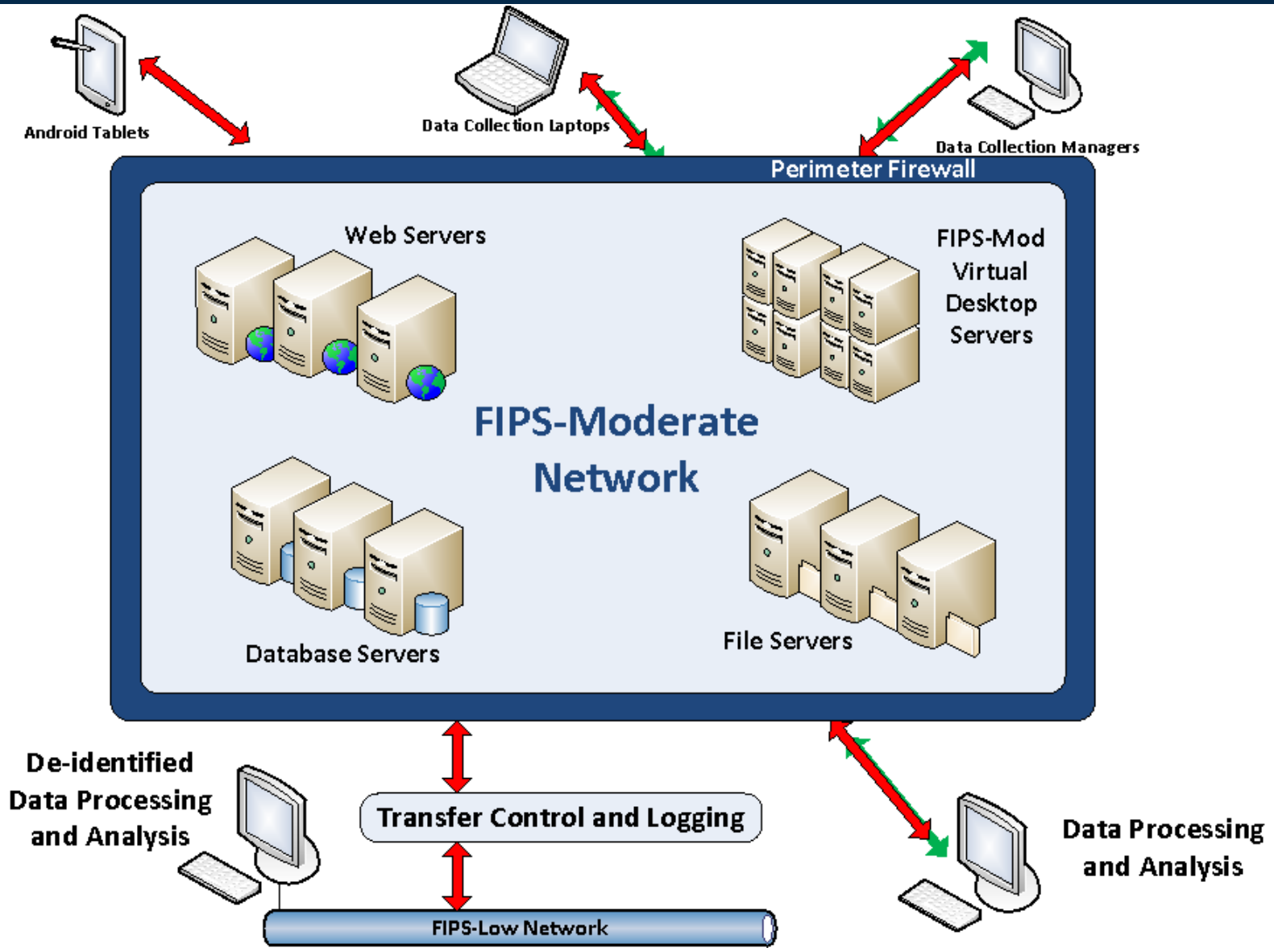
The Challenge!

- Make the necessary modifications and transition systems such that the NSDUH project will be compliant with FIPS-moderate requirements, and
- Complete all changes and obtain Authority to Operate (ATO) within 8 months.

Some key components:

- Solution needed that permitted SAMHSA to maintain data processing schedule to release First Findings Reports and Detailed Tables within 9 months post data collection
- Changes needed to data collection laptops and tablets to support multi-factor authentication and support remote laptop/tablet patching and antivirus updates
- Needed to modify contract to incorporate the changes to the IT system
- Needed to prepare and submit Authority to Operate (ATO) package for review and approval prior to targeted “go-live” date of November 2016 to ensure timely start to 2017 data collection (early January 5-6, 2017)

FIPS-Moderate Architecture and Data Flow

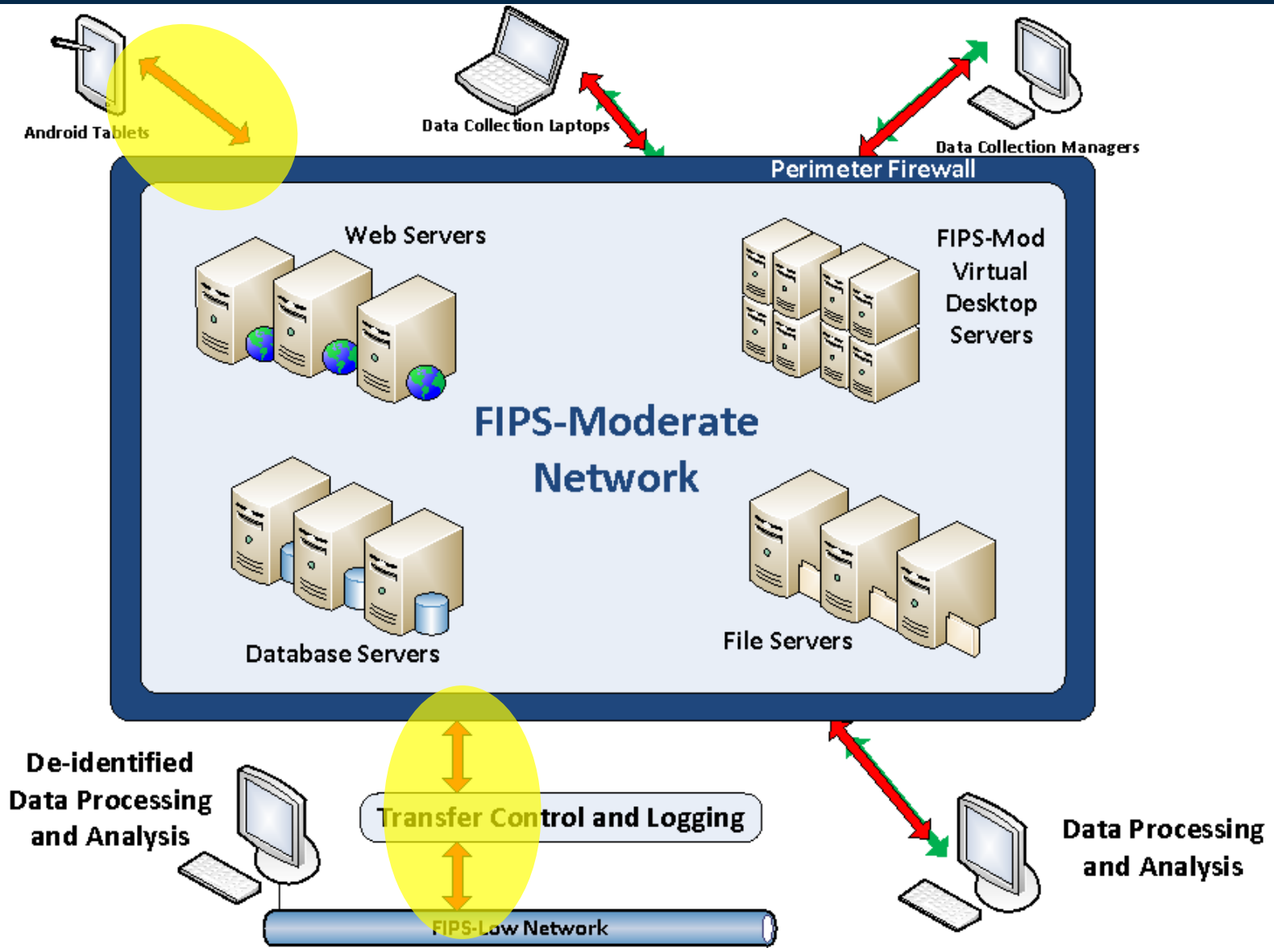


red arrow = encryption, green arrow = multifactor authentication

System Inventory – Pieces to Migrate to FIPS-Moderate

- Many moving pieces in the NSDUH support systems
- Websites and Web Servers
  - 2 Web Server Clusters
  - Informational Website for respondents and the general public
  - Case Management Website (used by supervisors and managers)
  - Intranet Website (used by data quality team, analysts, and developers)
  - File Sharing Repository
- Relational Databases (Websites and Data Management)
  - 2 Database Server clusters
  - ~ 40 SQL Server Databases
- Automatic Data Processing Workstations and Software
- File Storage
  - ~ 3 TB of data
- Desktops for Software Developers and Data Analysts
  - ~ 80 people

FIPS-Moderate Architecture and Data Flow

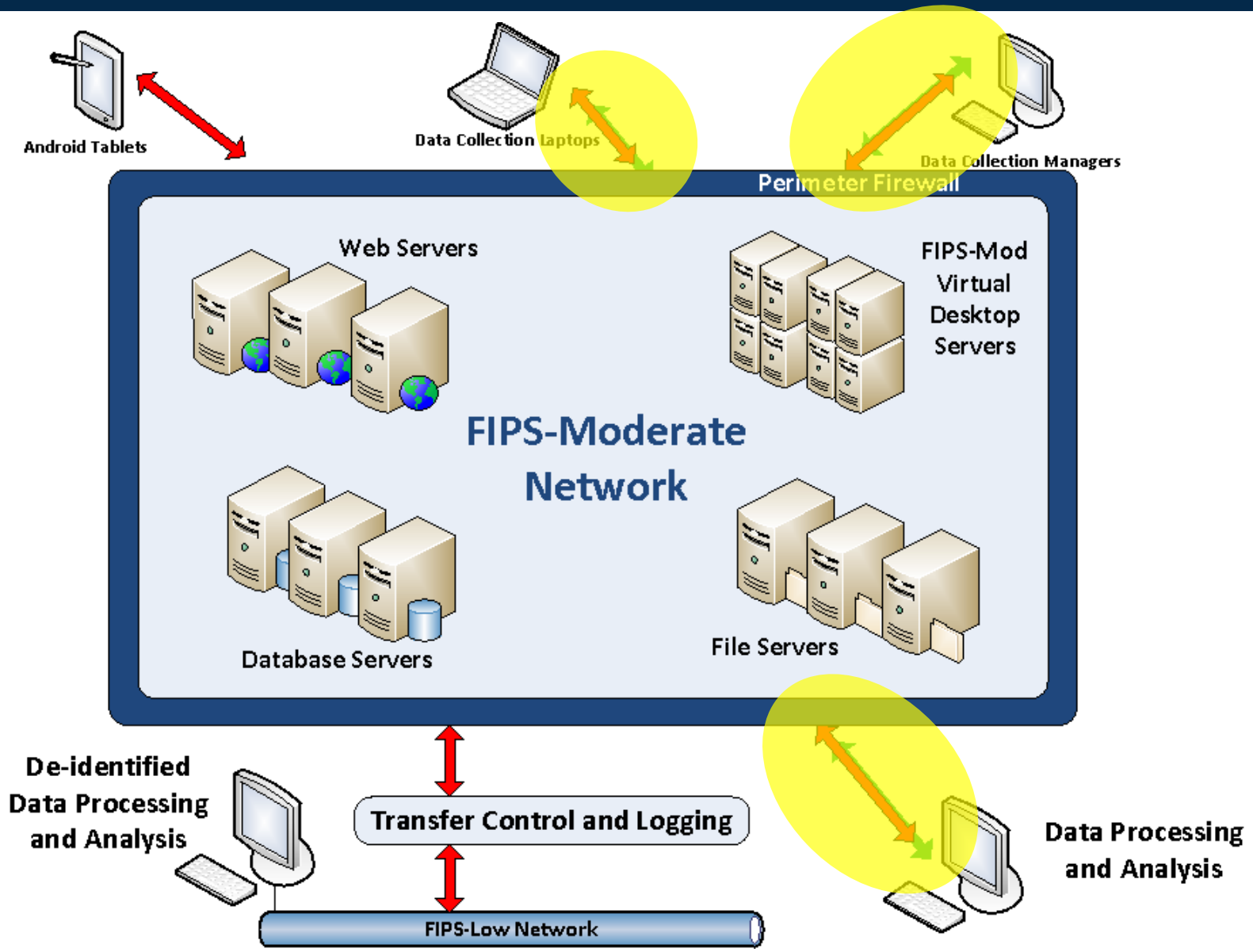


red arrow = encryption, green arrow = multifactor authentication

Encryption

- Requirement: Encryption methods used must comply with standards described in FIPS 140-2. Strong encryption algorithms.
- Data collection laptops (for NSDUH personal interview)
  - Device-level whole disk encryption
  - Separate encryption of completed interview files prior to transmission
- Data collection tablets (for NSDUH household screening)
  - Device level encryption of tablet memory
  - Separate attribute-level encryption of PII data items in app databases
- Transmission of Data To and From RTI
  - Transmission using encrypted protocols; SSL within HTTPS.
- Entry and Exit Points to the FIPS-Moderate Network
  - Encrypted FTP for all file transfers in and out; SFTP protocol
  - Only properly authenticated users can transfer files
  - All file transfers are logged
  - Interactions at system boundaries governed by ISAs.

FIPS Moderate System Architecture



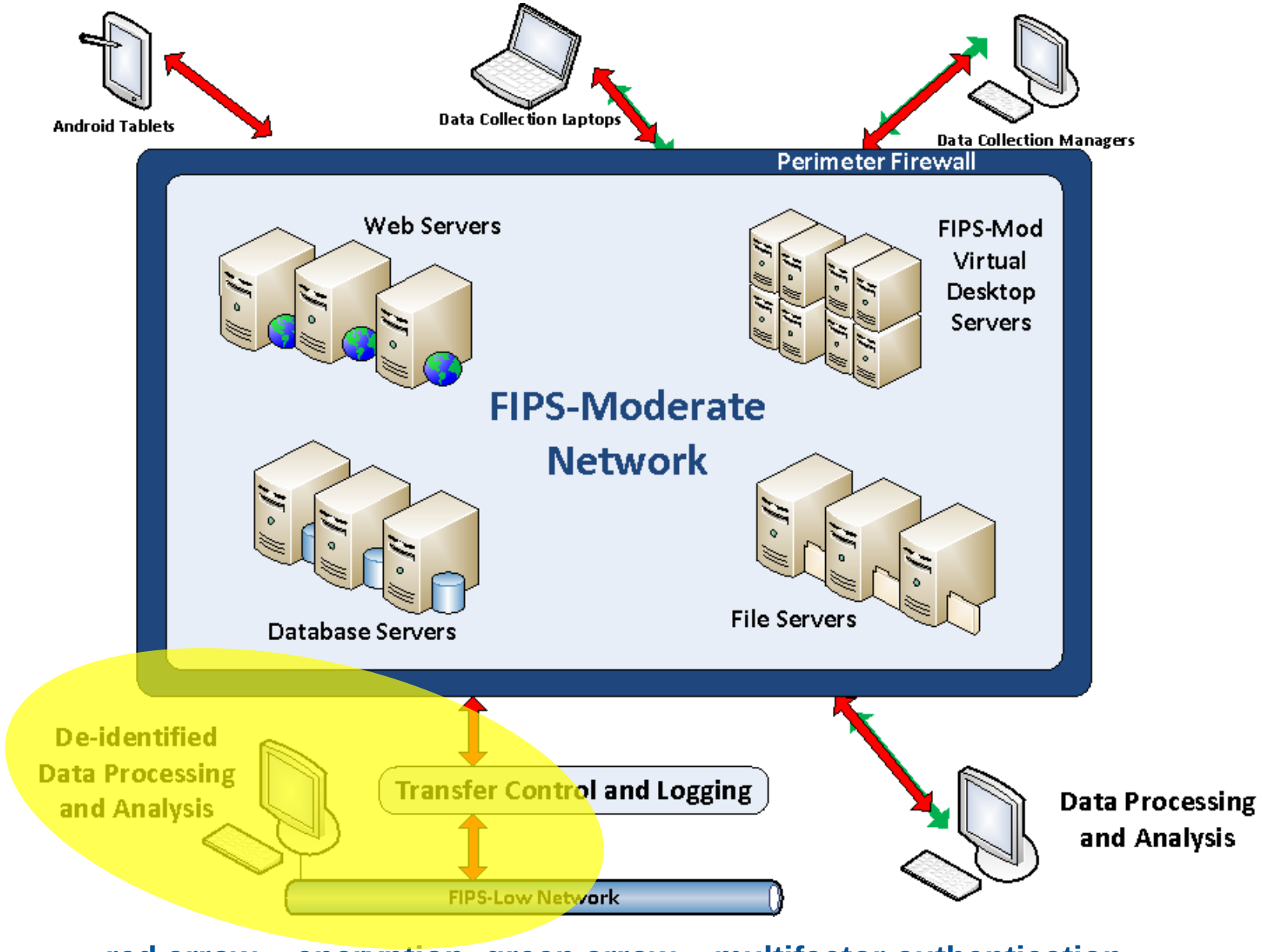
red arrow = encryption, green arrow = multifactor authentication

Multi-factor Authentication

- Sensitive information and PII must be secured using multi-factor
  - Something you know and something you have
- Network or internet connected devices
  - Standard OTP tokens like VASCO DIGIPASS and others
  - Users must supply a username/password and the token code
- Data collection laptops
  - Challenge … how to implement multi-factor in a disconnected environment? Unusual situation.
  - We selected the Yubikey solution from Yubico.
  - USB authentication key, including strong crypto and touch-to-sign, plus One-Time-Password, smart card, and FIDO U2F.
  - Laptops and Yubikeys uniquely paired.
  - Interviewers authenticate using Yubikeys and Windows username/password.

- Also used to secure the NSDUH case management web site.
- Interestingly – recently adopted by Facebook and Vanguard. Others …

FIPS Moderate System Architecture

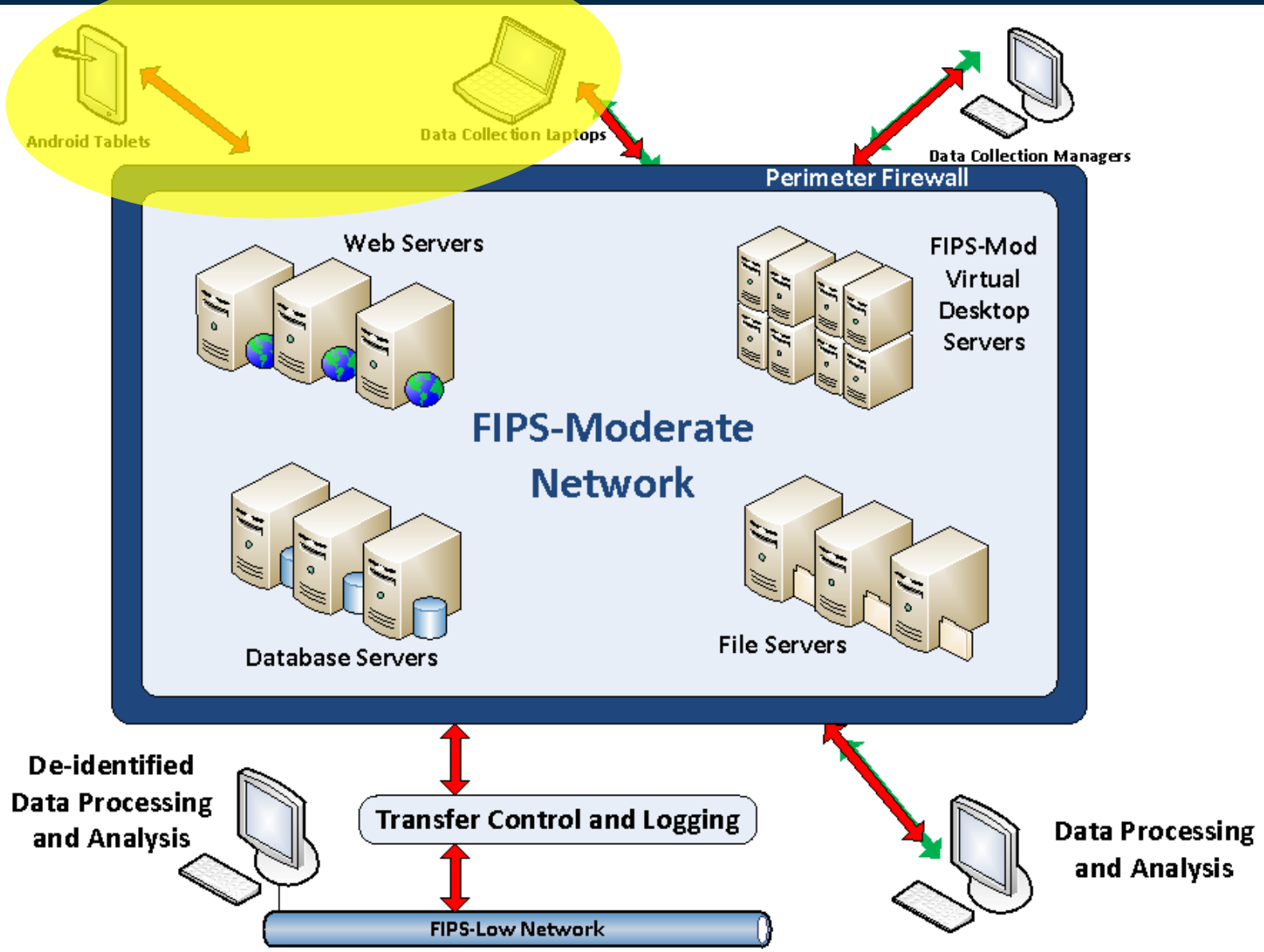


red arrow = encryption, green arrow = multifactor authentication

Data Processing

- Data files containing PII are restricted to the FIPS-Moderate zone.
- Working in a FIPS-Moderate environment, by design, is restrictive.
- Interaction with the outside world, other networks, and the internet are highly restricted or totally disallowed.
  - Example … copying and pasting text between emails and documents. Not in FIPS-Moderate!
  - Copying/pasting FIPS-Moderate source code, file locations or URLs to share with colleagues via email. Not in FIPS-Moderate!
- The more analysis we can do without including PII, the better off we are in terms of protecting participants' confidentiality.
- NSDUH approach is to appropriately de-identify data files prior to downstream data analysis.
  - PII is removed according to SAMHSA-provided guidelines.
  - Map between de-identified data and respondent demographics is maintained inside FIPS-Moderate environment.
  - Allows approximately 60% of data analysis to be done without needing PII, in a fully compliant properly authorized FIPS-Low environment.

FIPS Moderate System Architecture



red arrow = encryption, green arrow = multifactor authentication

Malicious Code Protection and Patching

- FIPS-Moderate specifies rigorous requirements for patching and anti-virus protection.
- For large fleet of disconnected data collection laptops and tablets (approx. 700 each) this is a big challenge.
- We are currently phasing in solutions for these requirements.
- Data collection laptops
  - LANDesk and McAfee EPO remote management for laptops
  - Patch distribution, antivirus software updating, remote auditing
  - Operational challenges due to lack of connectivity
- Data collection tablets
  - No existing commercial solution satisfies FIPS-Moderate requirements
  - RTI has developed a **Whitelist** solution for malicious code protection on the tablets.
    - Only allow a small set of apps known to be safe
    - Provide remote auditing capabilities
    - Ability to disable tablets that are out of compliance

Results So Far and Lessons Learned

- FIPS-Moderate system has been in production operation since November 2016.
- So far, the transition has been successful. No significant disruption of data collection due to increased security controls.
- Phasing in the laptop and tablet patching and AV protection is underway and ongoing. So far so good, but still some unknowns.
- For large studies like NSDUH, there is significant risk to manage.
  - Having a backup plan and being prepared for a thoughtful phased deployment is required.
  - Effective user training, field testing and advance planning are key activities in a transition of this type.
  - Multi-factor authentication has been a new training focus.
- Compared to collecting survey data under FIPS-Low, FIPS-Moderate is a bigger challenge. Hybrid solutions are attractive and can be designed to be FISMA-compliant.
- A word to the wise … Do not underestimate the effort that this kind of transition requires.

More Information

Peter Tice
NSDUH Project Officer
SAMHSA, CBHSQ
5600 Fishers Lane, 15E09D
Rockville, MD 20857
(240) 276-1254
Peter.Tice@samhsa.hhs.gov

David Hunter
NSDUH Project Director
RTI International
3040 East Cornwallis Road
Research Triangle Park, NC 27709
(919) 485-2612
dbc@rti.org

Marty Meyer
NSDUH Director of Data Security and Data Processing
RTI International
3040 East Cornwallis Road
Research Triangle Park, NC 27709
(919) 541-7035
mmeyer@rti.org