# NIAID VRO Progress Report

FIM4R Meeting 17FEB2020

@TIIME

Vienna, Austria

# This presentation

- Progress
- On-Prem Service Providers
- Off-Prem/Commercial SaaS Service Providers
- Challenges
  - science is scientists
- Next Steps
  - OIDC
  - Bulk identity and attribute operations
- The NIAID VRO MFA Project

# Current State of the NIAID VRO “On-Prem” and “Internal” Service Providers

- Remote Data Capture (5) – REDCap servers in Mali, Uganda, India, and AWS US East-1
- SharePoint Farms (3:2013, 1:2019) – AWS US East-1, NIAID, Data Center, Mali, and Uganda
- Moodle – (1) NIAID Data Center Rockville, MD
- Proconsul – (2) Uganda and AWS US East1
- Tableau – (1) AWS US East1
- HPC – (1) University of Science and Technology, Bamako, Mali

# Software-as-a-Service SPs

**Deployed**

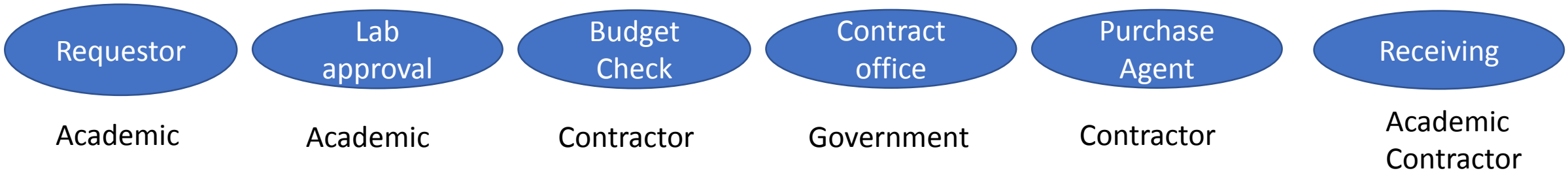
- Slack
- AWS Console

**Development**

- Box
- Meraki
- Office365
- Specimen Management

# Challenges
# Science is not just Scientists and Universities

- Research Contract Procurement Workflow
  - Academic IdP – Requestors
  - Government IdP – Approvers and Releasers
  - Office365 Tenant – contracted budget management
  - Office365 Tenant – contracted purchase agents
- Problems
  - Contractors unfamiliar with the use of federated credentials
  - SharePoint InfoPath Forms
  - SharePoint



# Social Identities

- Cirrus Identity
  - Google (gmail and g-suite)
  - Microsoft (Office365, Hotmail, MSN, Outlook.com)
  - LinkedIn
  - Yahoo (?)

# Next steps

- Satosa OIDC (in addition to SAML2)
- Bulk Operations
  - Bulk enrollments
  - Bulk group management
  - Use of the Comanage API for
- Switch from OpenLDAP to AD LDS
- MFA

# The NIAID VRO MFA Project

- User accesses an SP in the NIAID VRO
- The NIAID VRO SP (Satosa) requests authentication context from IdPs
- The AuthN from the IdP signals SFA or MFA under Refeds Assurance Framework
- If no MFA or no context provided the user receives an MFA from the service integrated with Satosa
- In addition to the MFA credential the user session also receives attributes from the comanage directory for consumption by the SP

# Problem with the MFA Project

- Nobody seems to know what happens when an SP requests Authentication context of IdPs in the broader trust federation community
- Solution – test (particularly the SaaS and COTS IdPs)
- Build an SP that is placed into the InCommon and eduGAIN Metadata
- The SP (perhaps a wiki) configured to request AuthContext and consume with verbose logs
- Publicize to the federated identity community and ask them to test access and report
- Collect the data and report to next FIM4R

# Acknowledgments

Mike Tartakovsky NIAID CIO
Jeff Erickson NIH IAM
Matt Eisenberg NIAID OCICB
Spherical Cows
Internet2 InCommon
Geant
REFEDS
FIM4R Community
LIGO

FIN