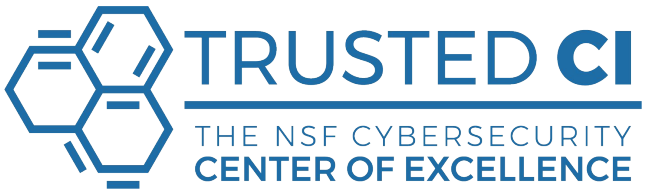
U.S. ARF / CICoE Pilot / Trusted CI Identity Management (IdM) Engagement

John Haverlack
R/V Sikuliaq
College of Fisheries and Ocean Sciences
University of Alaska Fairbanks

Josh Drake
Ci CoE Pilot/Trusted CI
Indiana University Center for Applied Cybersecurity Research

Ryan Kiser
Trusted CI
Indiana University Center for Applied Cybersecurity Research



UNIVERSITY OF ALASKA FAIRBANKS
R/V Sikuliaq
College of Fisheries and Ocean Sciences
https://www.sikuliaq.alaska.edu

ARF IdM Engagement Plan

https://docs.google.com/document/d/1Btb4VRaXrZzg_8brZ_viSMy20PNH-AlcTnamwwr22Ss/edit

May - October 2020

- **Milestone 1:** Catalog Current State of IdM in the ARF
- **Milestone 2:** Recommend an IdM solution
- **Milestone 3:** Proof of concept IdM solution

UNIVERSITY OF ALASKA FAIRBANKS

R/V Sikuliaq

College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CI CoE PILOT

CFOS

UNOLS

NSF

Objectives of a Federated IdM Service

This engagement explored how to:

- Provide an Opt-In per vessel per service IdM Solution
- Centralized Identity Management capability for the Fleet
- Facilitate Auditability of Authentication Events
- Monitor expired or inactive accounts for deactivation
- Reduce use of shared password accounts
- Leverage Institutional Identity Providers rather than creating new identities
- Streamline On/Off Boarding Processes
- Develop a Shipside Authentication Appliance

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT

UAF UNIVERSITY OF ALASKA FAIRBANKS
R/V Sikuliaq
College of Fisheries and Ocean Sciences
https://www.sikuliaq.alaska.edu

CFOS
UNIVERSITY OF ALASKA FAIRBANKS Seward, AK R/V SIKULIAQ
UNIVERSITY NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM UNOLS
NSF

IdM Primer Video

IdM Primer Video
https://youtu.be/rZWOXeOsN6E

IdM Primer Presentation
https://docs.google.com/presentation/d/1_riLUbkQYiqvOsPXezn3GLwehj1WEWLwfiELo4qwxiE/edit?usp=sharing

- Authentication
- Authorization
- Authentication Services
- Auditability
- Shared Accounts
- Federated Identity Services

Milestone 1: State of IdM in US ARF - Survey Results

- 10 Institution Responded / 15 Vessels Represented
- 60% don't know how many Institute accounts are accessed each year
- 50% don't know how many Transient accounts are accessed each year
- 80% don't know how many inactive accounts are enabled
- Shared Password Roll Accounts are commonly used
- Majority of Credentials are managed locally on each device
- A small number of vessels use AD/LDAP
- End users are storing passwords insecurely
- 60% have only local system logs / 20% have centralized logging
- 10% regularly audit logs
- Majority require strong passwords / 30% use 2FA
- There is a mix of processes for adding / removing accounts

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT

UAF UNIVERSITY OF ALASKA FAIRBANKS
R/V Sikuliaq
College of Fisheries and Ocean Sciences
https://www.sikuliaq.alaska.edu

CFOS
UNIVERSITY OF ALASKA FAIRBANKS Seward, AK R/V SIKULIAQ
UNIVERSITY NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM UNOLS
NSF

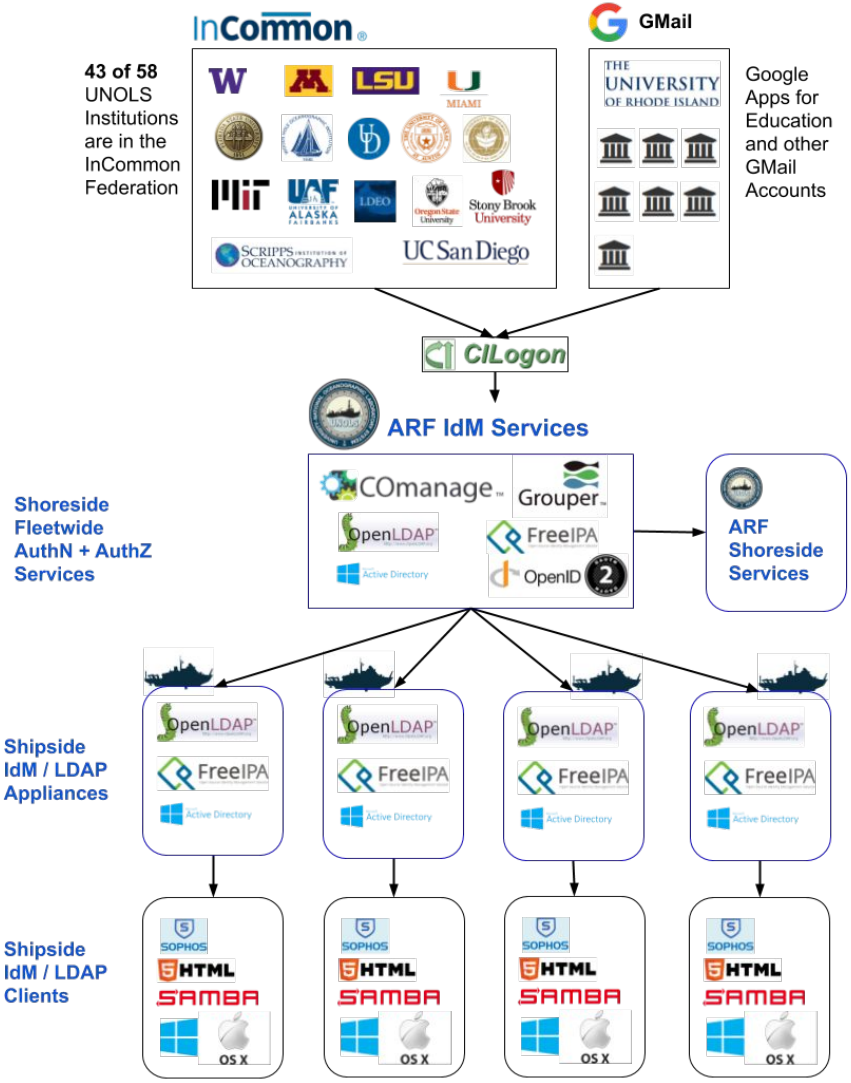
Milestone 1: State of IdM in US ARF

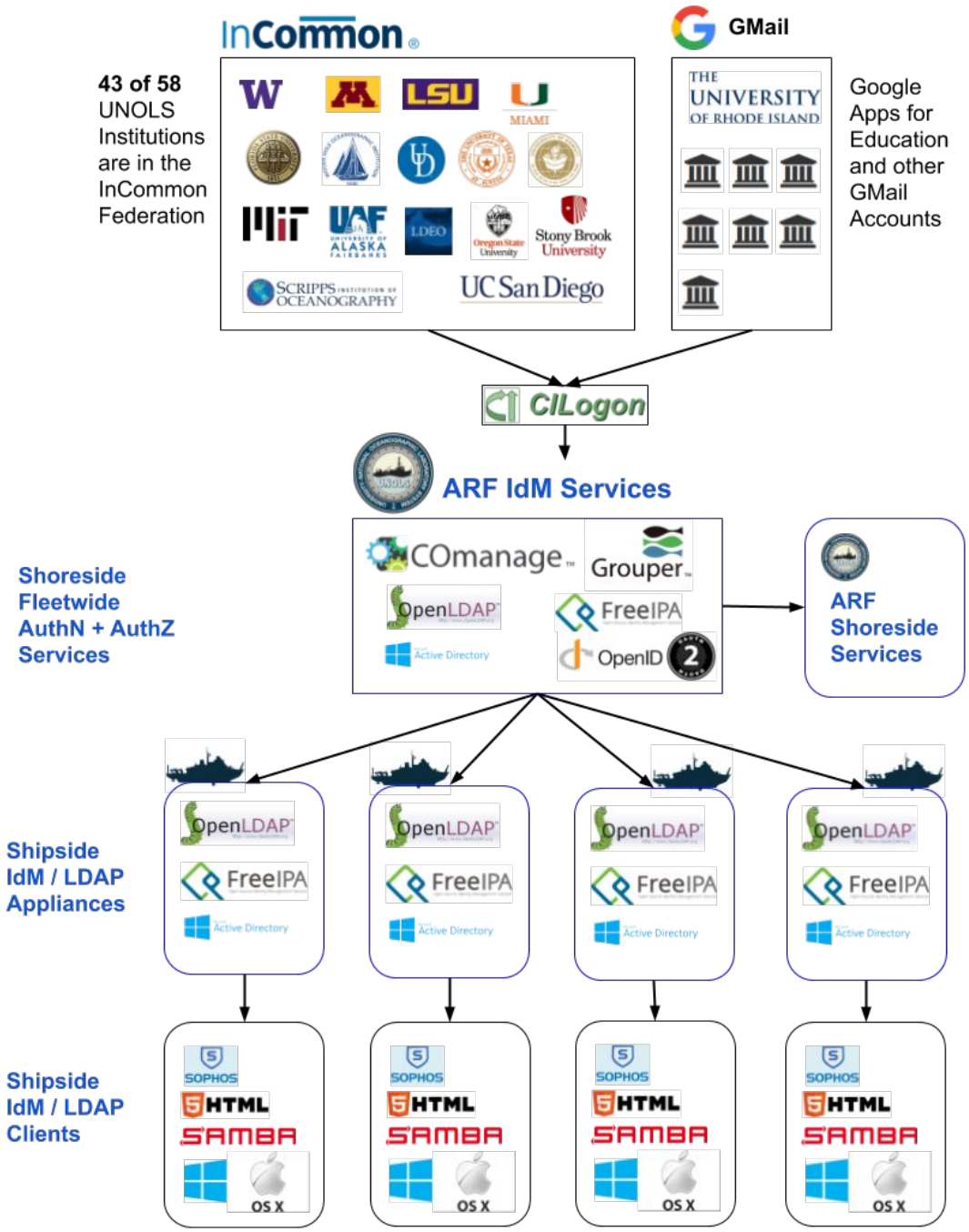
Survey Respondents:

- Support Federated IdM for Cruise Planning, Captive Portal, Science Logging, and File Sharing
- Are mixed or do not support Federated IdM for Email, Kiosks, VDI, SysAdmin, Ops Tech, Vessel Maintenance
- Agree that Federated IdM should never block logins if the Internet is down
  Strongly desire the ability to administer identities from vessel networks
- Agree that federated IdM will be opt-in on a per vessel per service basis

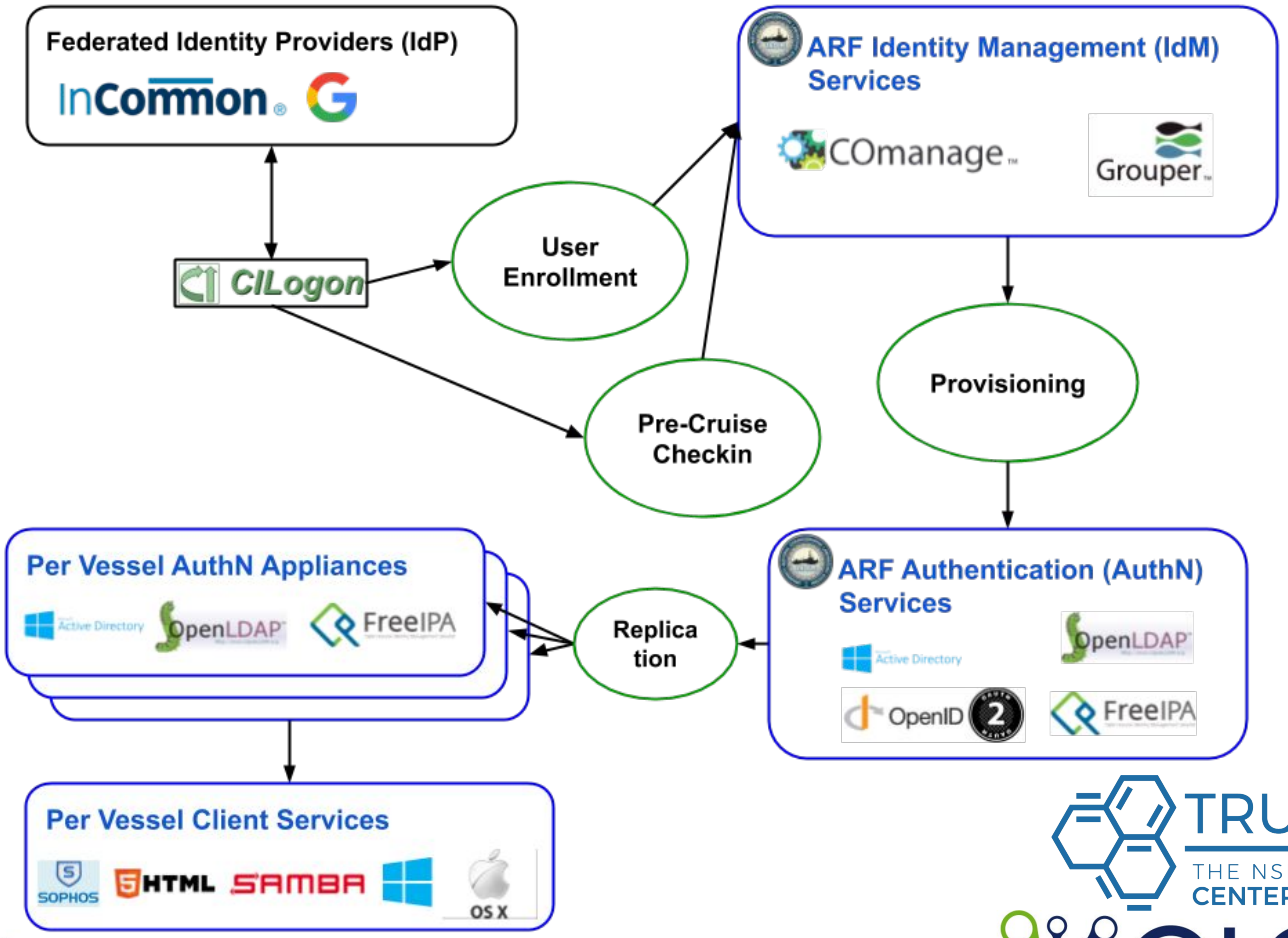
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT

Milestone 2: Recommended Solution




InCommon
43 of 58 UNOLS Institutions are in the InCommon Federation
GMail
Google Apps for Education and other GMail Accounts
CILogon
ARF IdM Services
COmanage
Grouper
OpenLDAP
FreeIPA
Active Directory
OpenID
Shoreside Fleetwide AuthN + AuthZ Services
ARF Shoreside Services
Shipside IdM / LDAP Appliances
Shipside IdM / LDAP Clients
SOPHOS
HTML
SAMBA
OS X

IdM Workflow



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT

UNIVERSITY OF ALASKA FAIRBANKS

R/V Sikuliaq

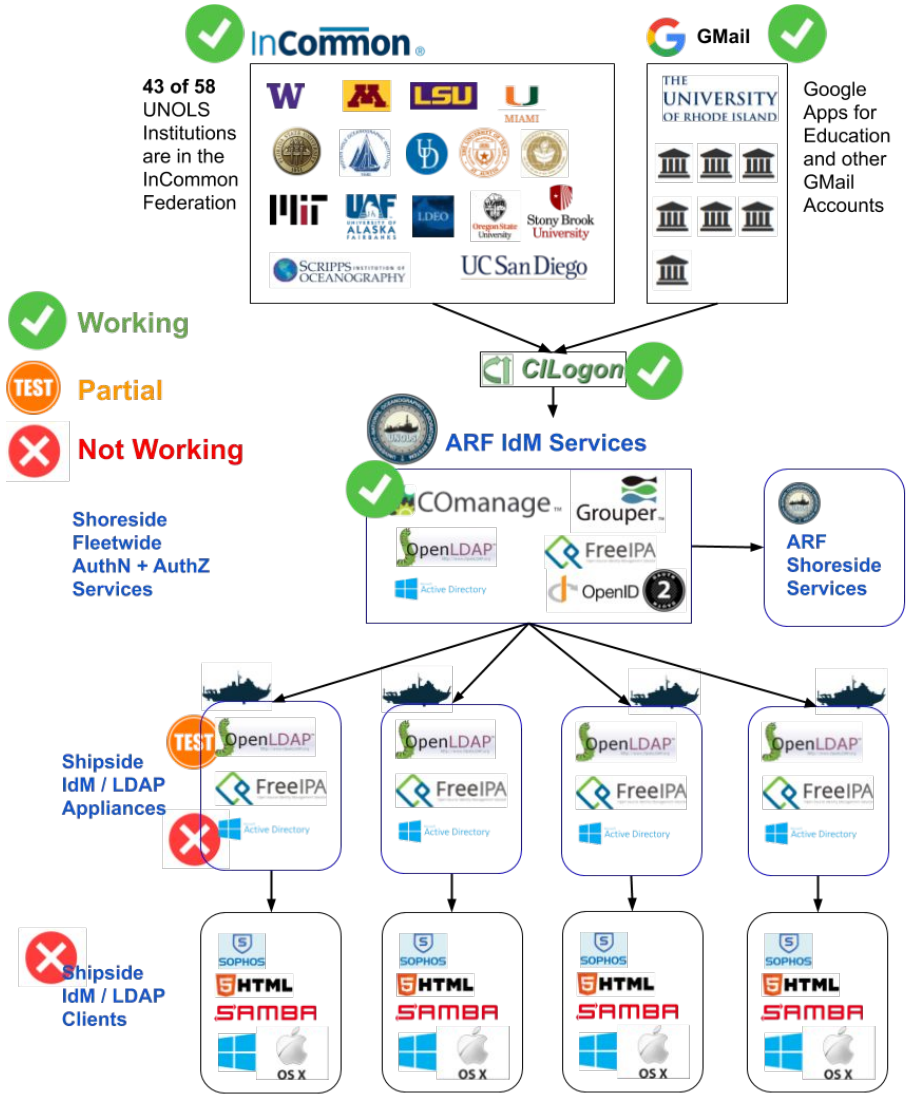
College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

Milestone 3:
Proof of Concept

How far did we get?

- Working InCommon / Google Federation
- Working ARF COManage Instance
- Partial Open LDAP Server
- Incomplete AD Server
- Incomplete Samba Client

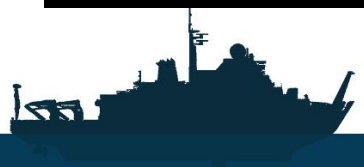


COmanage™ CILogon

Federated Authentication

https://drive.google.com/file/d/1-fXr5xxzAQ6m55ng5FYc6R0UKfgTwHsS/view?usp=sharing

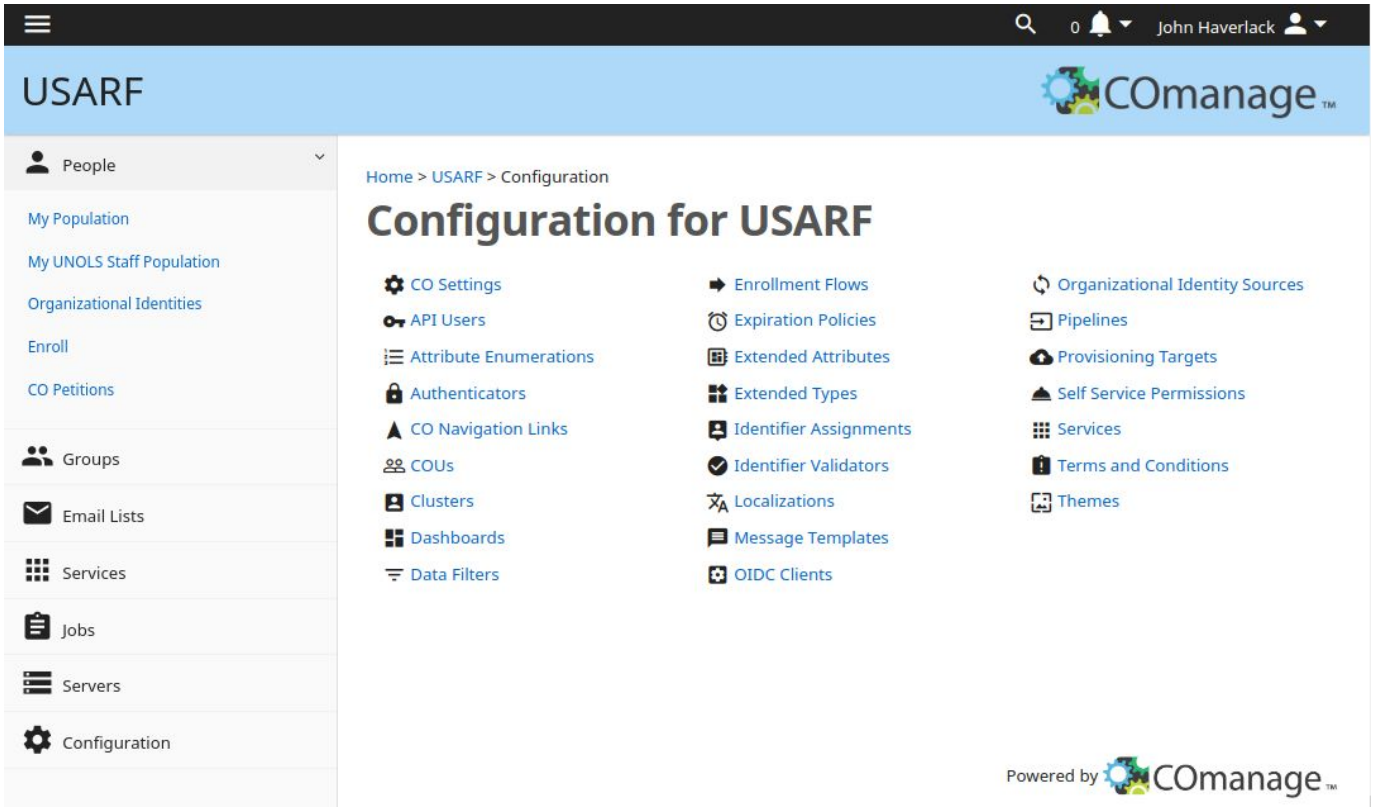
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT



UNIVERSITY OF ALASKA FAIRBANKS
R/V Sikuliaq
College of Fisheries and Ocean Sciences
https://www.sikuliaq.alaska.edu

CFOS
UNIVERSITY OF ALASKA FAIRBANKS Seward, AK R/V SIKULIAQ
UNIVERSITY NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM UNOLS
NSF

COmanage™



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CI CoE PILOT

UAF UNIVERSITY OF ALASKA FAIRBANKS

R/V Sikuliaq

College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

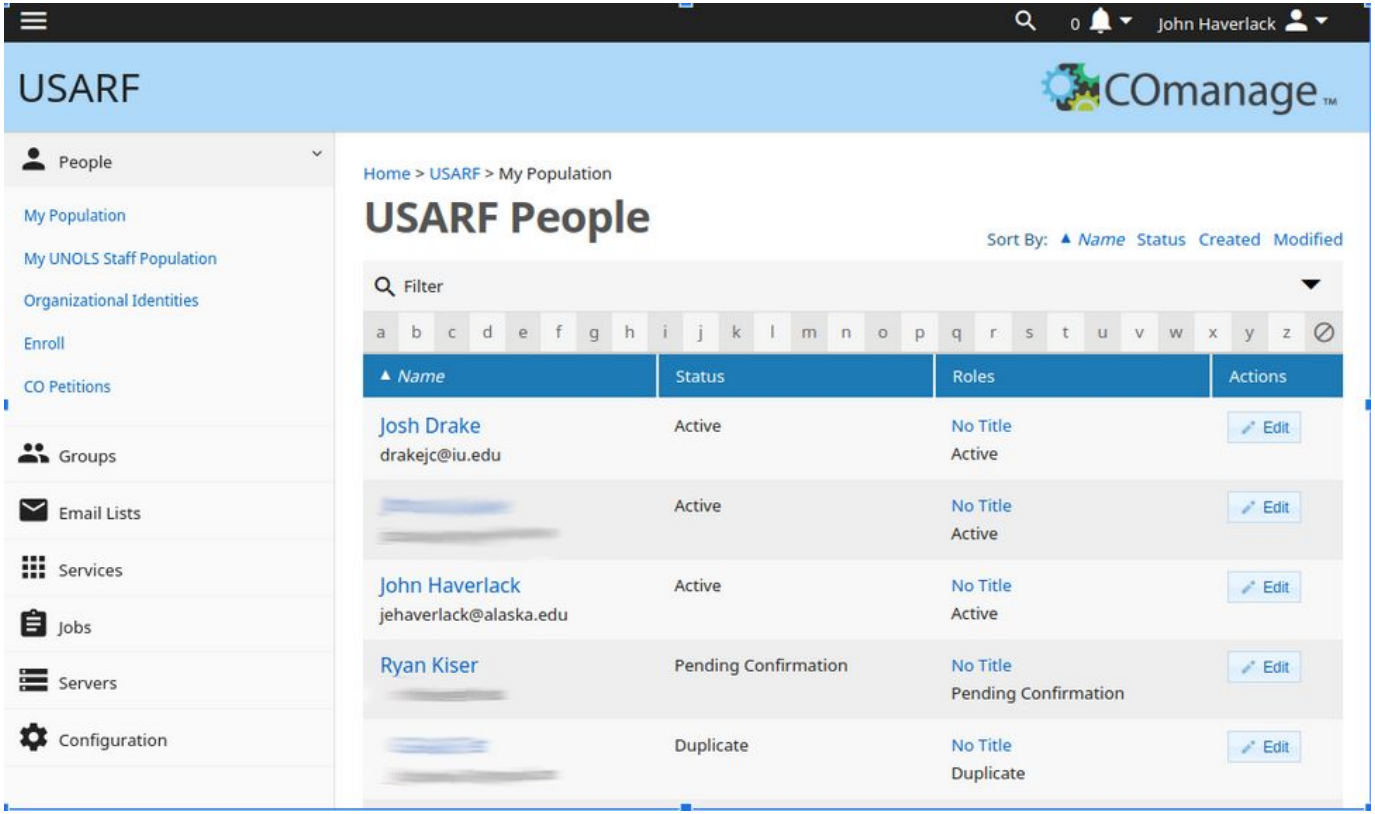
CFOS

UNIVERSITY OF ALASKA FAIRBANKS Seward, AK R/V SIKULIAQ

UNIVERSITY NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM UNOLS

NSF

COmanage™



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CI CoE PILOT

UAF UNIVERSITY OF ALASKA FAIRBANKS

R/V Sikuliaq

College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

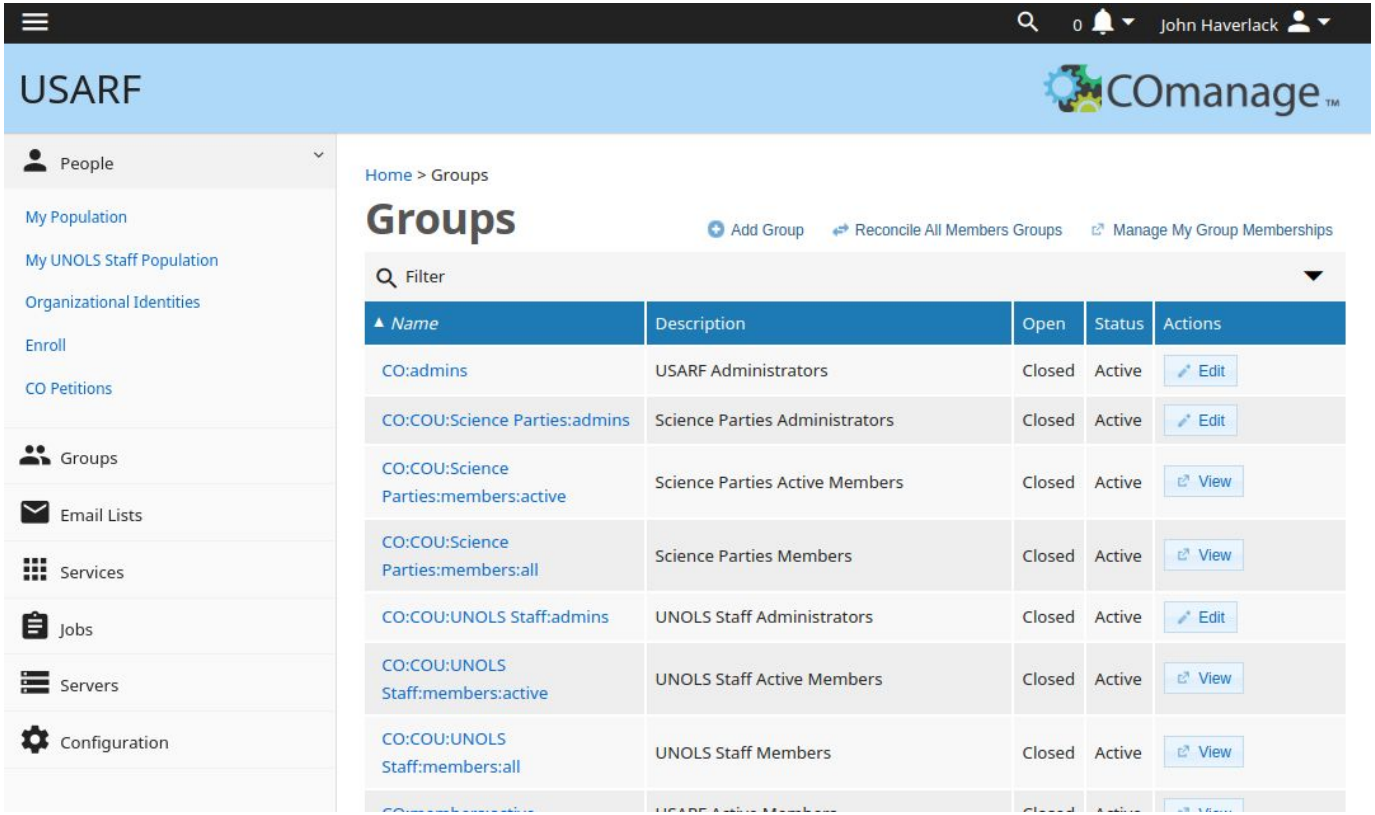
CFOS

UNIVERSITY OF ALASKA FAIRBANKS · Seward, AK · R/V SIKULIAQ

UNIVERSITY NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM · UNOLS

NSF

COmanage™



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT

UAF UNIVERSITY OF ALASKA FAIRBANKS

R/V Sikuliaq

College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

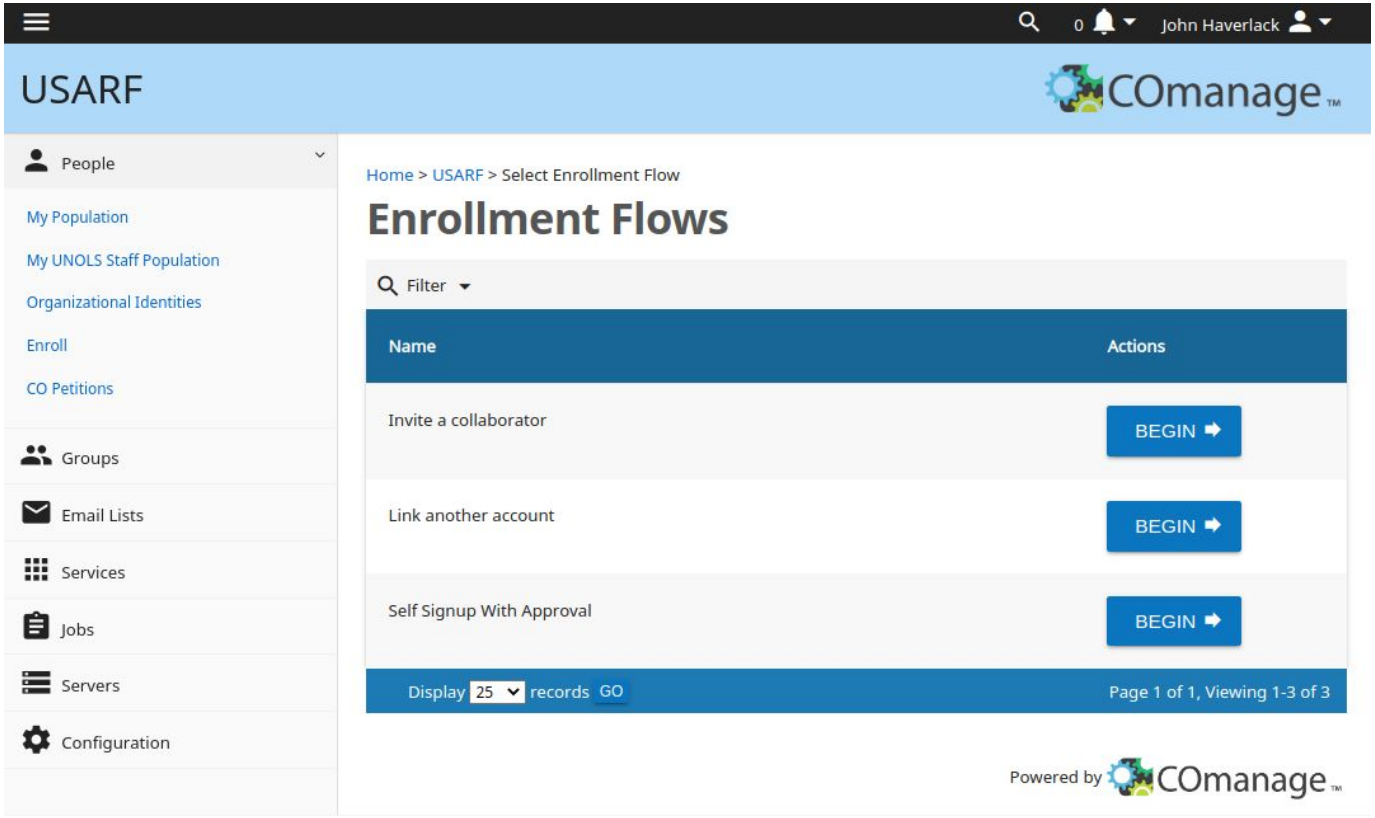
CFOS

UNIVERSITY OF ALASKA FAIRBANKS Seward, AK R/V SIKULIAQ

UNIVERSITY NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM UNOLS

NSF

COmanage™



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT

UNIVERSITY OF ALASKA FAIRBANKS

R/V Sikuliaq

College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

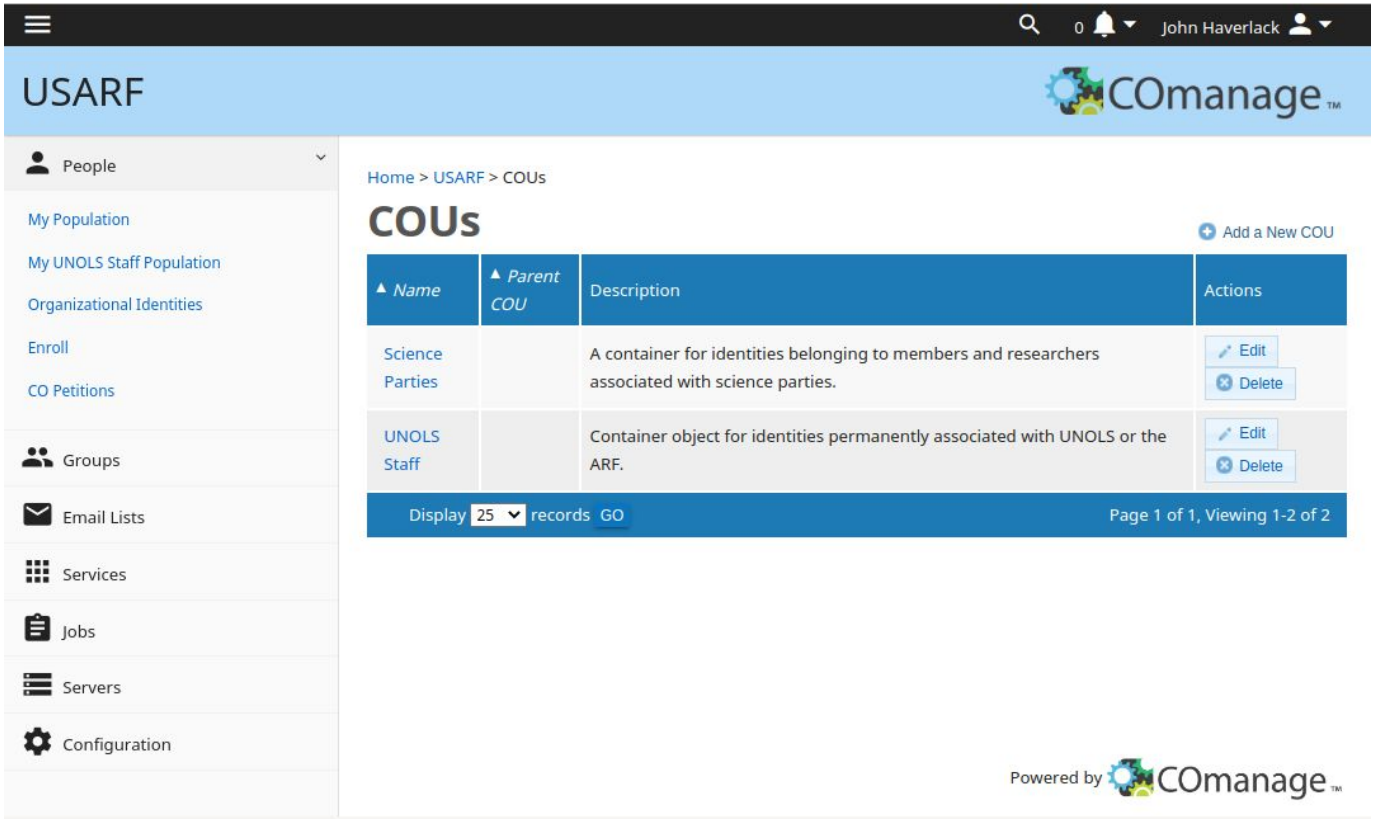
CFOS

UNIVERSITY OF ALASKA FAIRBANKS · Seward, AK · R/V SIKULIAQ

UNIVERSITY NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM · UNOLS

NSF

COmanage™



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT

UNIVERSITY OF ALASKA FAIRBANKS

R/V Sikuliaq

College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

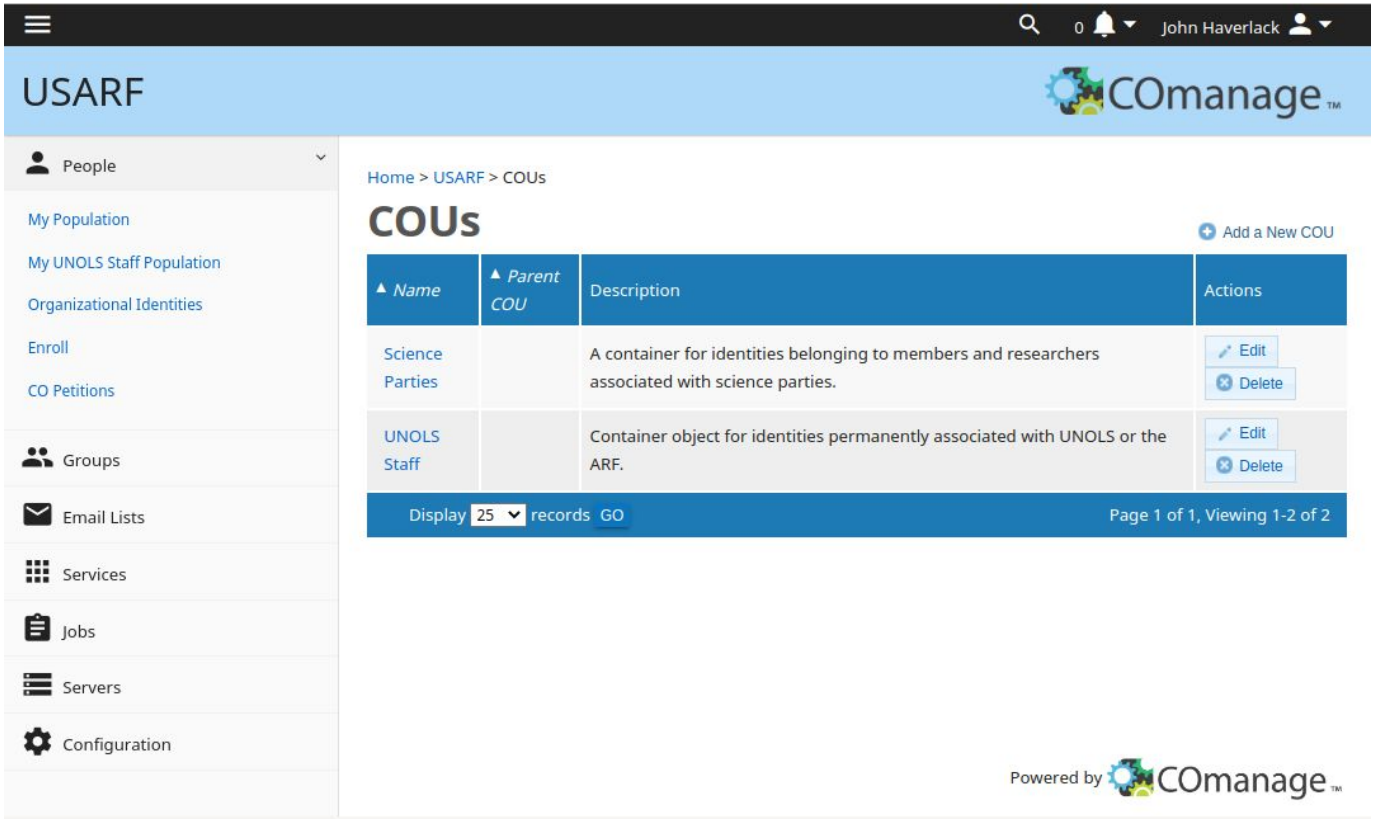
CFOS

UNIVERSITY OF ALASKA FAIRBANKS · Seward, AK · R/V SIKULIAQ

UNIVERSITY NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM · UNOLS

NSF

COmanage™



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT

UNIVERSITY OF ALASKA FAIRBANKS

R/V Sikuliaq

College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

CFOS

UNIVERSITY OF ALASKA FAIRBANKS · Seward, AK · R/V SIKULIAQ

UNIVERSITY NATIONAL OCEANOGRAPHIC LABORATORY SYSTEM · UNOLS

NSF

Challenges

- Identity Management is Complicated
- There is more than one way to organize identity data
- Integrating authentication systems is hard
- Bi-directional administration (ship to shore) is not currently available
- CILogon annual subscription: ~$9,000 per year

There are resources that can help us.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT

CFOS
UNOLS
NSF

Next Steps

- Write a **Federated Identity Management Service** Proposal
  - Available to U.S. ARF on a **per vessel / per service Opt-In** basis
  - Would pursue potential collaborations with
    - CILogon
    - CICoE
    - Trusted CI
    - Marine Facilities Planner (IdM Client)
  - Request funding to establish and run IdM service for 5 years

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
CI CoE PILOT