CyberCAT

Cyber Control Assessment Tool

James [redacted]

Section 5125 | August 1, 2024

Jet Propulsion Laboratory
California Institute of Technology

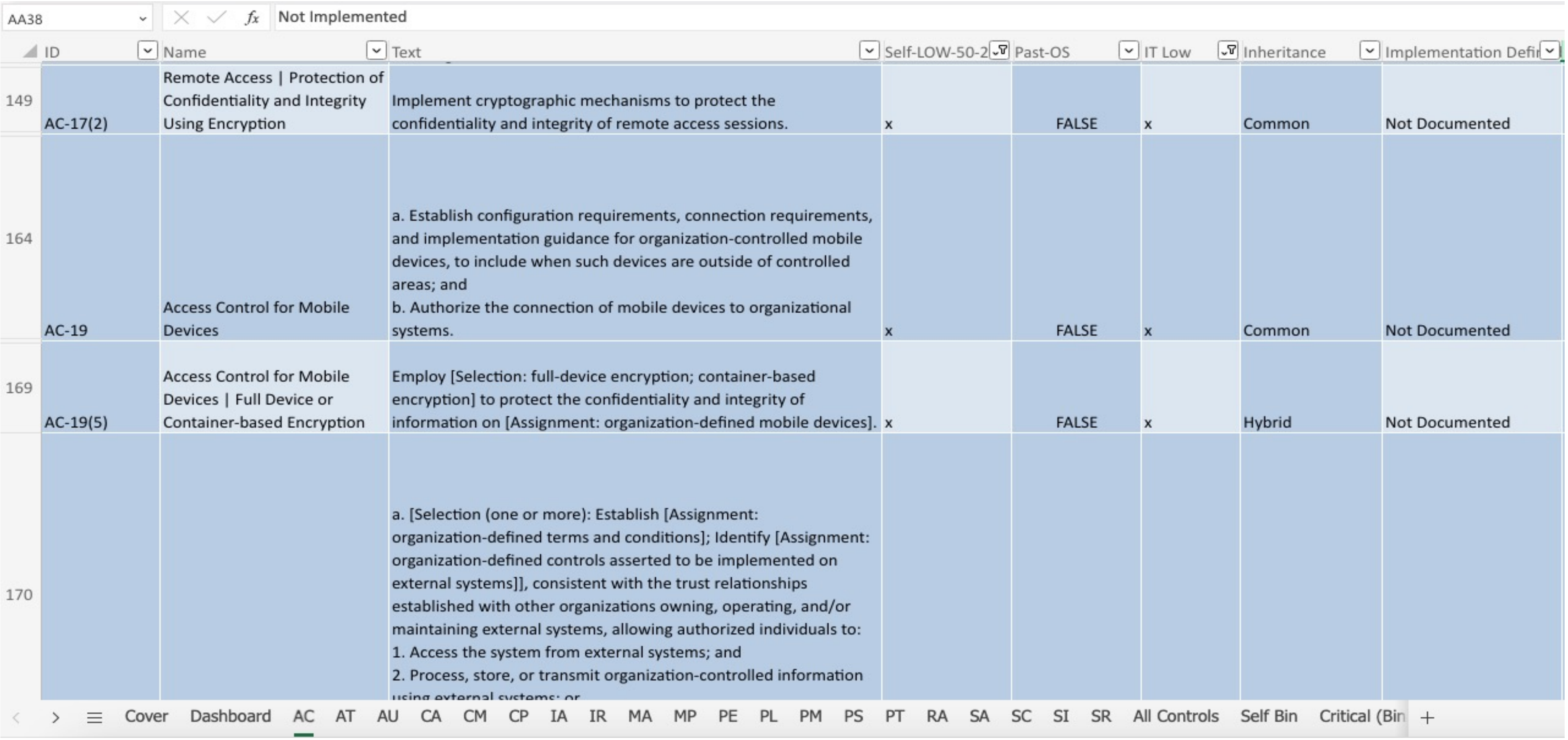
Agenda

- [redacted]
- Project Background
- Cyber Control Assessment Tool (CyberCAT)
  - Project Goals
  - Contributions
  - Challenges Overcome
  - Current State of the Project
- Learning Outcomes
- Acknowledgements

Background - The Problem

Conducting cybersecurity assessments takes time

- Assessments include hundreds of requirements (from NIST 800-53 controls)
- Assessments vary in requirements to be evaluated
- Assessments require working with systems, stakeholders, and documents
- Current tools are outdated and not user-friendly



AA38 *fx* Not Implemented

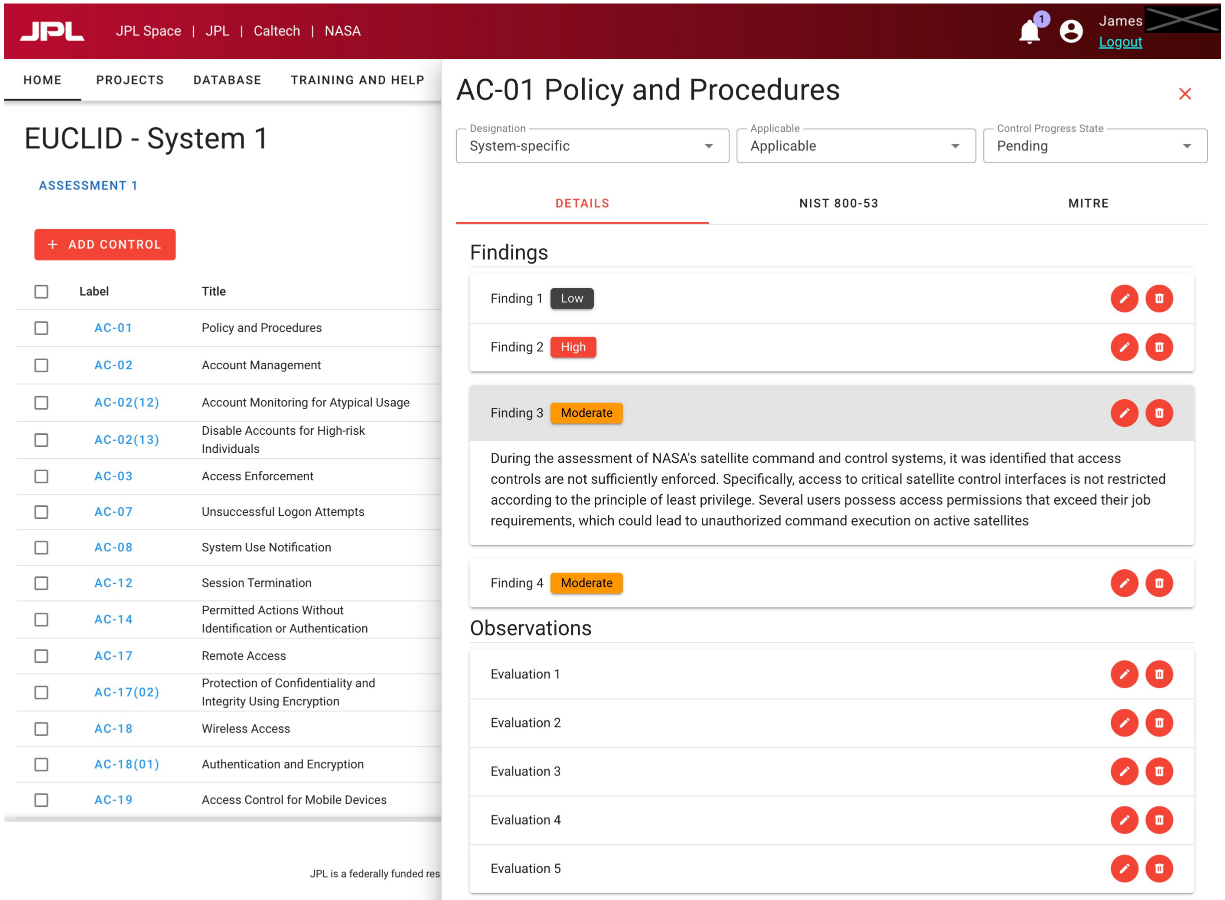
	ID	Name	Text	Self-LOW-50-2	Past-OS	IT Low	Inheritance	Implementation Defi
149	AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	x	FALSE	x	Common	Not Documented
164	AC-19	Access Control for Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.	x	FALSE	x	Common	Not Documented
169	AC-19(5)	Access Control for Mobile Devices | Full Device or Container-based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].	x	FALSE	x	Hybrid	Not Documented
170			a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or					

CyberCAT – The Solution

Cyber Control Assessment Tool

CyberCAT helps assessors conduct assessments

- Proof-of-concept completed prior to my arrival
- Brings together all the steps of conducting assessments into a single interface
- Produce first production version by the end of my internship



EUCLID - System 1

□	Label	Title
□	AC-01	Policy and Procedures
□	AC-02	Account Management
□	AC-02(12)	Account Monitoring for Atypical Usage
□	AC-02(13)	Disable Accounts for High-risk Individuals
□	AC-03	Access Enforcement
□	AC-07	Unsuccessful Logon Attempts
□	AC-08	System Use Notification
□	AC-12	Session Termination
□	AC-14	Permitted Actions Without Identification or Authentication
□	AC-17	Remote Access
□	AC-17(02)	Protection of Confidentiality and Integrity Using Encryption
□	AC-18	Wireless Access
□	AC-18(01)	Authentication and Encryption
□	AC-19	Access Control for Mobile Devices

JPL is a federally funded res

AC-01 Policy and Procedures

Designation: System-specific
Applicable: Applicable
Control Progress State: Pending

Findings

Finding 1 Low

Finding 2 High

Finding 3 Moderate

During the assessment of NASA's satellite command and control systems, it was identified that access controls are not sufficiently enforced. Specifically, access to critical satellite control interfaces is not restricted according to the principle of least privilege. Several users possess access permissions that exceed their job requirements, which could lead to unauthorized command execution on active satellites

Finding 4 Moderate

Observations

Evaluation 1

Evaluation 2

Evaluation 3

Evaluation 4

Evaluation 5

CyberCAT – Project, Team, and Goals

What do we need before assessors can start using it?

- Team
  - **James** [redacted] - Developer
  - Cristopher H[redacted] – Mentor, Lead Developer
  - Steven [redacted] G[redacted] – User Experience Designer
  - James M[redacted] – Co-Mentor, Stakeholder

- Implementation Goals:
  - Login with JPL credentials
  - Create Assessments
  - Track Progress
  - Record Findings
  - Review reference material

Completed Milestones

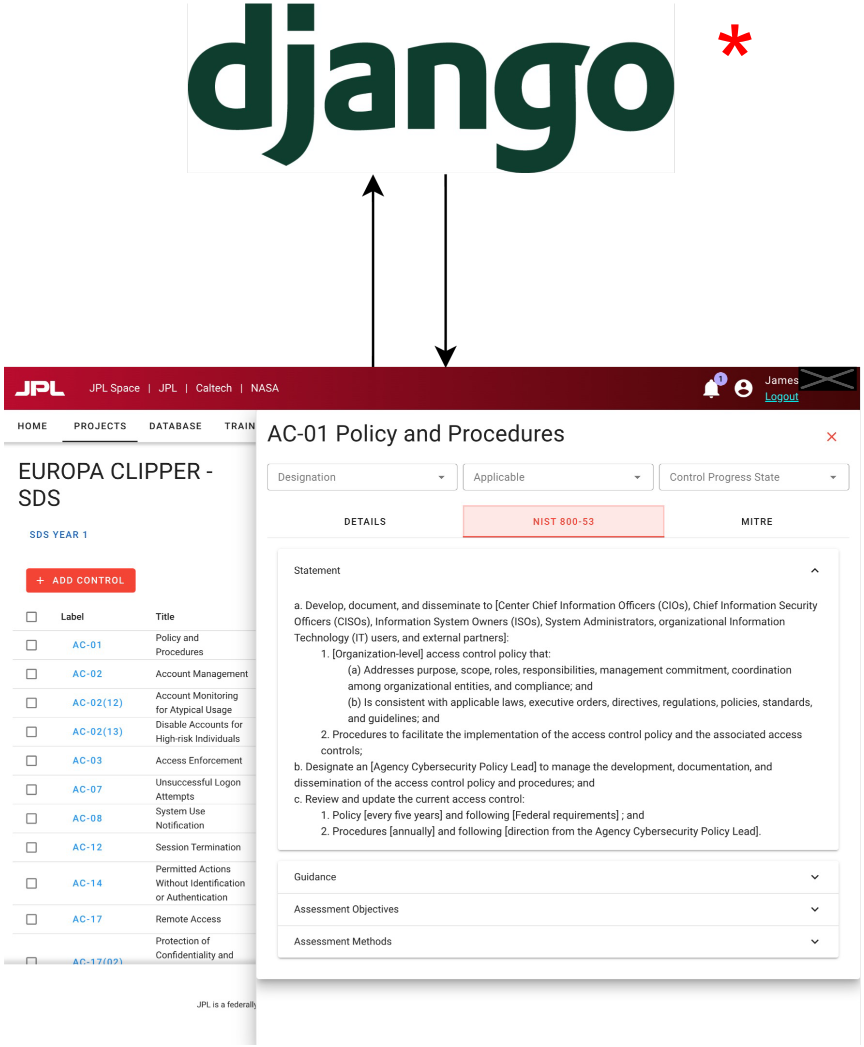
- CyberCAT tested with working assessors
- Automated Testing with Django Rest Framework
- Designed and Implemented User Experience in collaboration with Steve (UX Designer) and stakeholders
- Developmental Features
  - Login with JPL Account
  - Create Customized Assessments
  - View controls associated with assessments
  - Bulk modify assessments
  - Record findings and assessor notes

Lessons Learned

- Working with UX designer is new for me!
- When external parties are a part of a project (Cloud Services), it can slow down a project’s deployment
- CyberCAT’s deployment was not seamless due to changes in how the frontend connects to the backend

Software

- **Frontend**: Vue.js and Vuetify
  - JavaScript-based visual frameworks to build interactive user interfaces that are easy to use
- **Backend**: Django + Django Rest Framework
  - Python-based frameworks which handles the processing and storage of all data which goes through CyberCAT



James [redacted]
Logout

EUROPA CLIPPER - SDS

SDS YEAR 1

☐	Label	Title
☐	AC-01	Policy and Procedures
☐	AC-02	Account Management
☐	AC-02(12)	Account Monitoring for Atypical Usage
☐	AC-02(13)	Disable Accounts for High-risk Individuals
☐	AC-03	Access Enforcement
☐	AC-07	Unsuccessful Logon Attempts
☐	AC-08	System Use Notification
☐	AC-12	Session Termination
☐	AC-14	Permitted Actions Without Identification or Authentication
☐	AC-17	Remote Access
☐	AC-17(02)	Protection of Confidentiality and

JPL is a federally

AC-01 Policy and Procedures

Statement

a. Develop, document, and disseminate to [Center Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Information System Owners (ISOs), System Administrators, organizational Information Technology (IT) users, and external partners]:

1. [Organization-level] access control policy that:
   (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

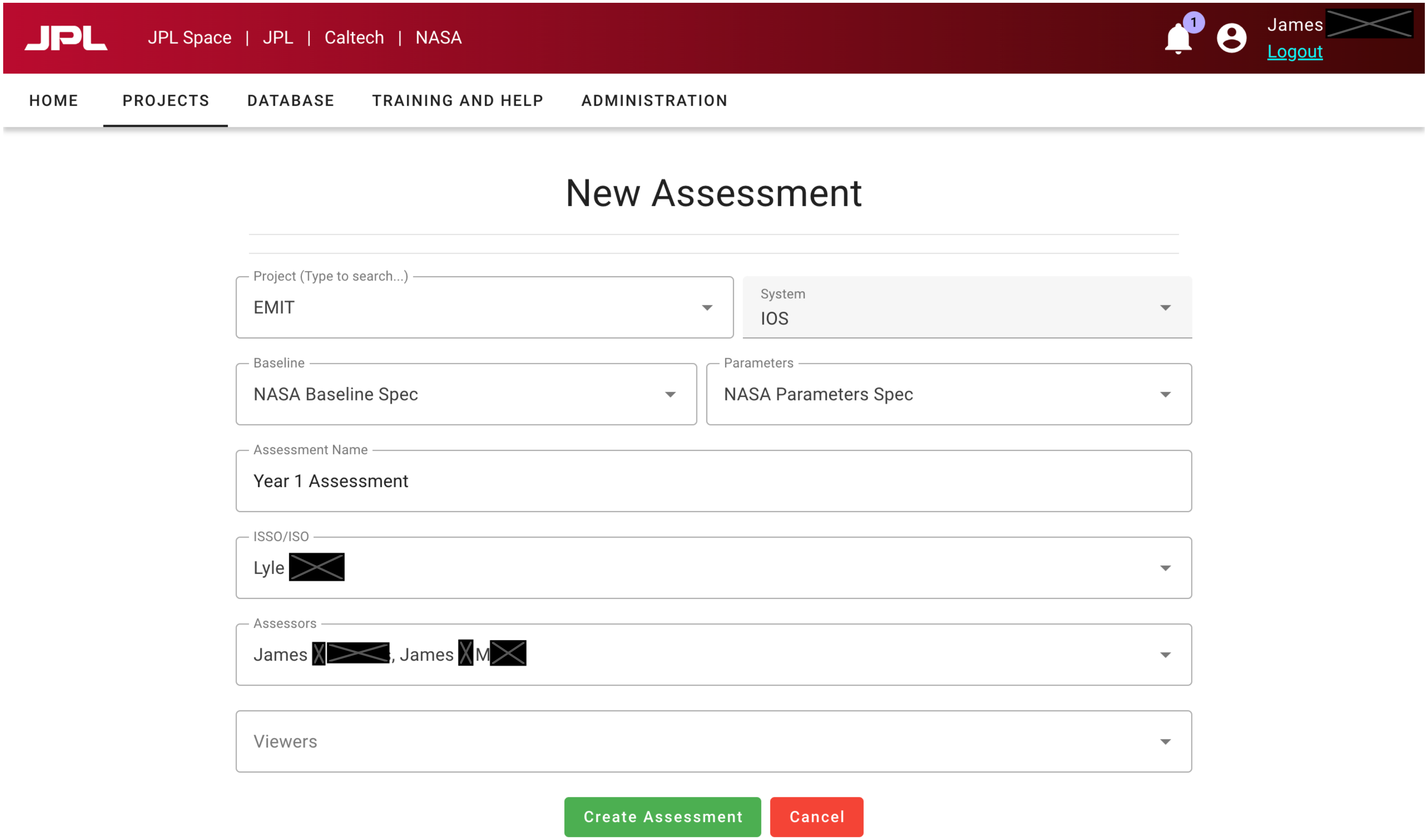
b. Designate an [Agency Cybersecurity Policy Lead] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy [every five years] and following [Federal requirements] ; and
2. Procedures [annually] and following [direction from the Agency Cybersecurity Policy Lead].

* Django logo used for software platform identification only, this project is not officially endorsed by the Django Project (https://www.djangoproject.com/).
(image source: https://www.djangoproject.com/community/logos/)

CyberCAT - Assessments



New Assessment

Project (Type to search...): EMIT

System: IOS

Baseline: NASA Baseline Spec

Parameters: NASA Parameters Spec

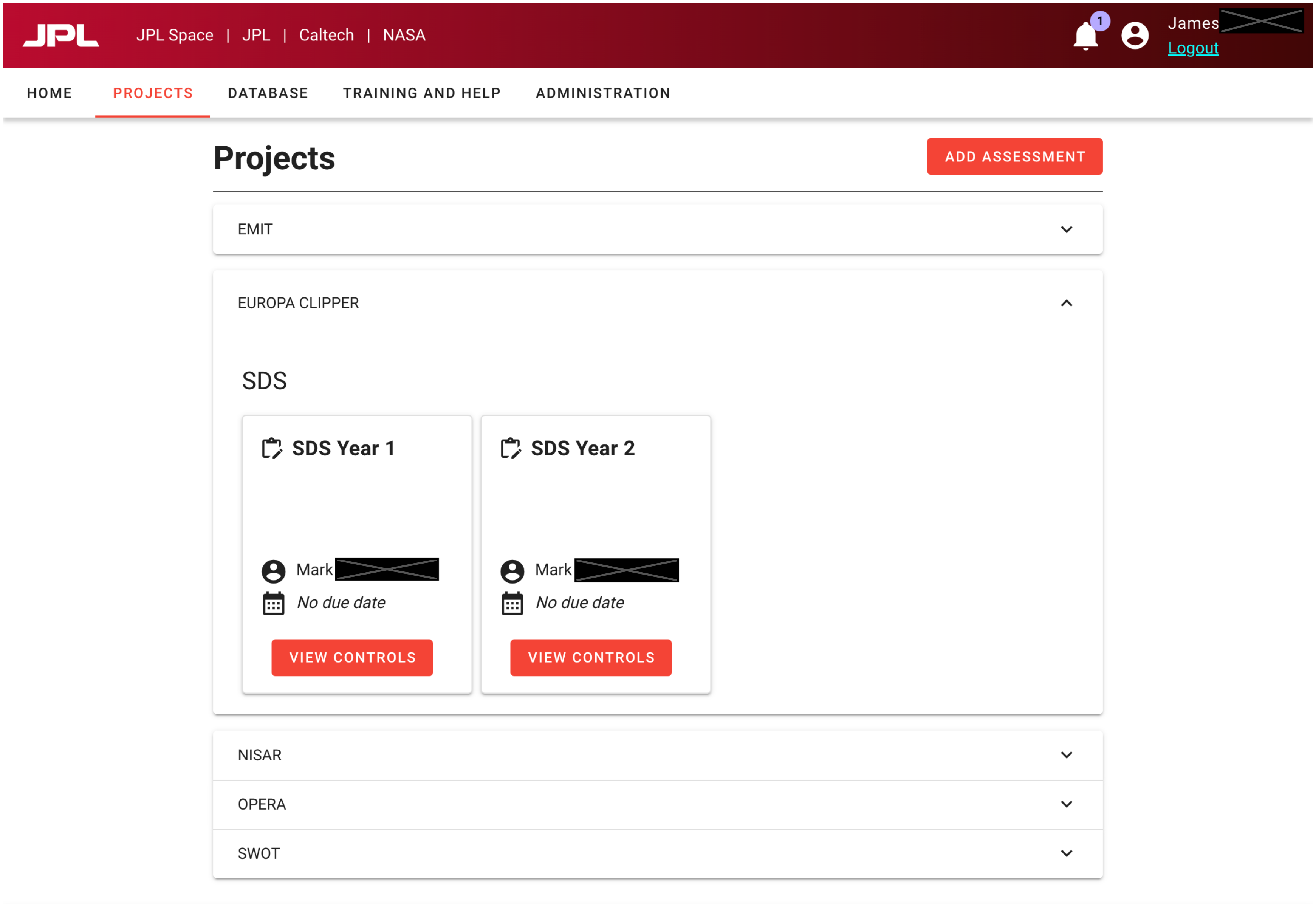
Assessment Name: Year 1 Assessment

ISSO/ISO: Lyle [redacted]

Assessors: James [redacted], James [redacted]M[redacted]

Viewers

CyberCAT – Projects



Projects

EMIT

EUROPA CLIPPER

SDS

SDS Year 1

Mark [redacted]

No due date

SDS Year 2

Mark [redacted]

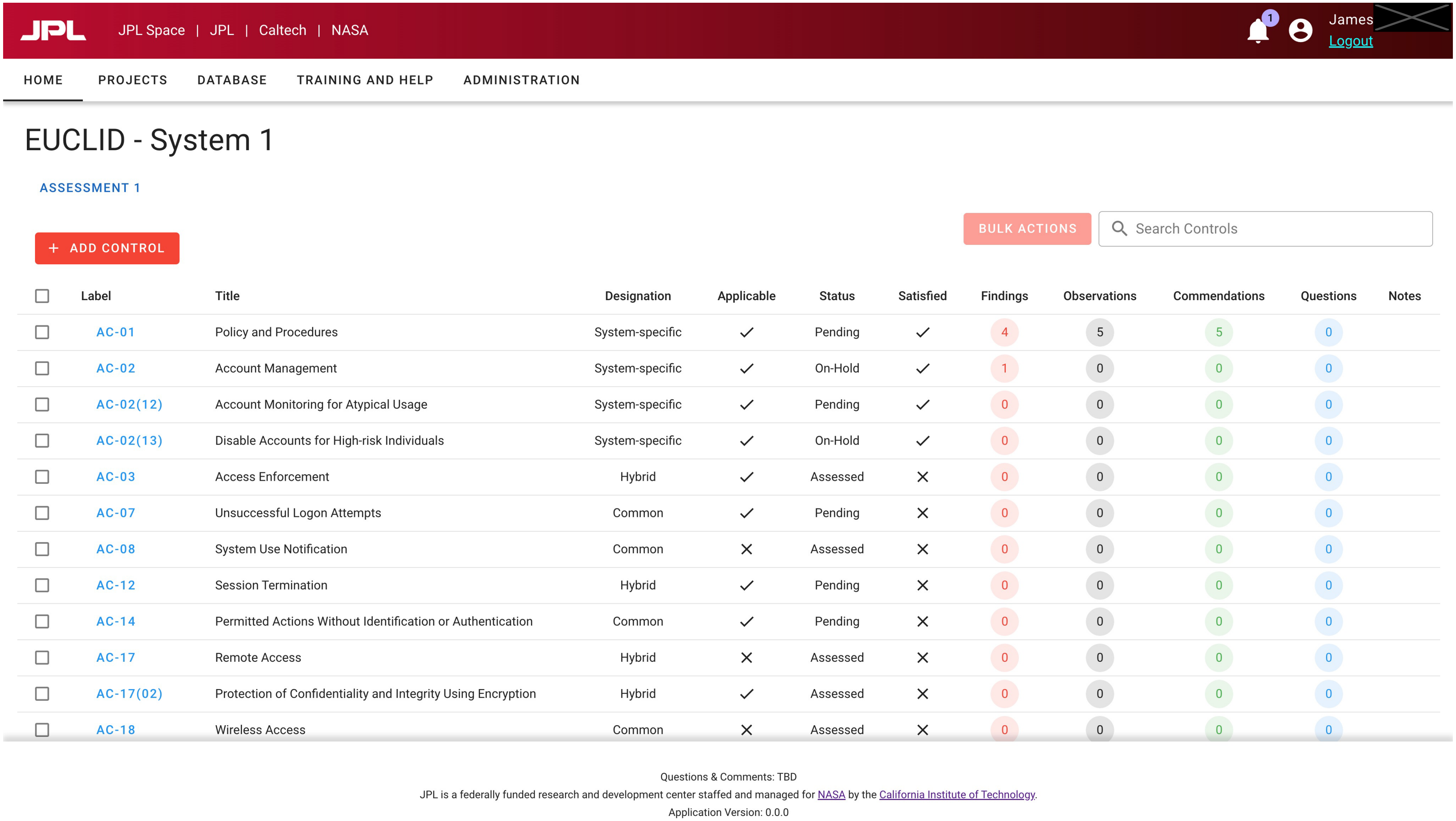
No due date

NISAR

OPERA

SWOT

Assessment Interface



EUCLID - System 1

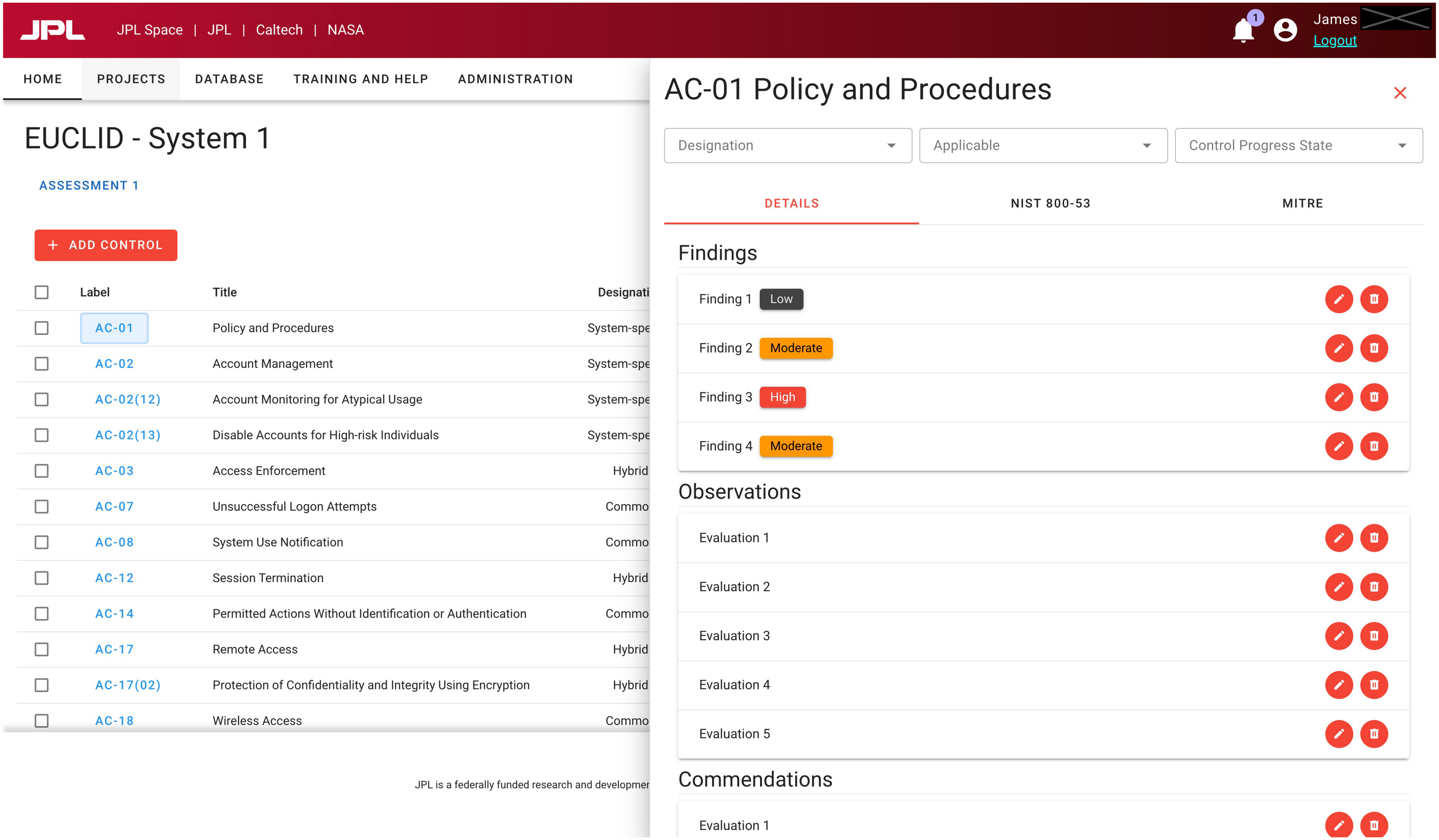
□	Label	Title	Designation	Applicable	Status	Satisfied	Findings	Observations	Commendations	Questions	Notes
□	AC-01	Policy and Procedures	System-specific	✓	Pending	✓	4	5	5	0	
□	AC-02	Account Management	System-specific	✓	On-Hold	✓	1	0	0	0	
□	AC-02(12)	Account Monitoring for Atypical Usage	System-specific	✓	Pending	✓	0	0	0	0	
□	AC-02(13)	Disable Accounts for High-risk Individuals	System-specific	✓	On-Hold	✓	0	0	0	0	
□	AC-03	Access Enforcement	Hybrid	✓	Assessed	✗	0	0	0	0	
□	AC-07	Unsuccessful Logon Attempts	Common	✓	Pending	✗	0	0	0	0	
□	AC-08	System Use Notification	Common	✗	Assessed	✗	0	0	0	0	
□	AC-12	Session Termination	Hybrid	✓	Pending	✗	0	0	0	0	
□	AC-14	Permitted Actions Without Identification or Authentication	Common	✓	Pending	✗	0	0	0	0	
□	AC-17	Remote Access	Hybrid	✗	Assessed	✗	0	0	0	0	
□	AC-17(02)	Protection of Confidentiality and Integrity Using Encryption	Hybrid	✓	Assessed	✗	0	0	0	0	
□	AC-18	Wireless Access	Common	✗	Assessed	✗	0	0	0	0	

Questions & Comments: TBD

JPL is a federally funded research and development center staffed and managed for NASA by the California Institute of Technology.

Application Version: 0.0.0

Control Interface - Details



EUCLID - System 1

□	Label	Title	Designati
□	AC-01	Policy and Procedures	System-spe
□	AC-02	Account Management	System-spe
□	AC-02(12)	Account Monitoring for Atypical Usage	System-spe
□	AC-02(13)	Disable Accounts for High-risk Individuals	System-spe
□	AC-03	Access Enforcement	Hybrid
□	AC-07	Unsuccessful Logon Attempts	Commo
□	AC-08	System Use Notification	Commo
□	AC-12	Session Termination	Hybrid
□	AC-14	Permitted Actions Without Identification or Authentication	Commo
□	AC-17	Remote Access	Hybrid
□	AC-17(02)	Protection of Confidentiality and Integrity Using Encryption	Hybrid
□	AC-18	Wireless Access	Commo

JPL is a federally funded research and developmer

AC-01 Policy and Procedures

Designation ▾ | Applicable ▾ | Control Progress State ▾

Findings

- Finding 1 Low
- Finding 2 Moderate
- Finding 3 High
- Finding 4 Moderate

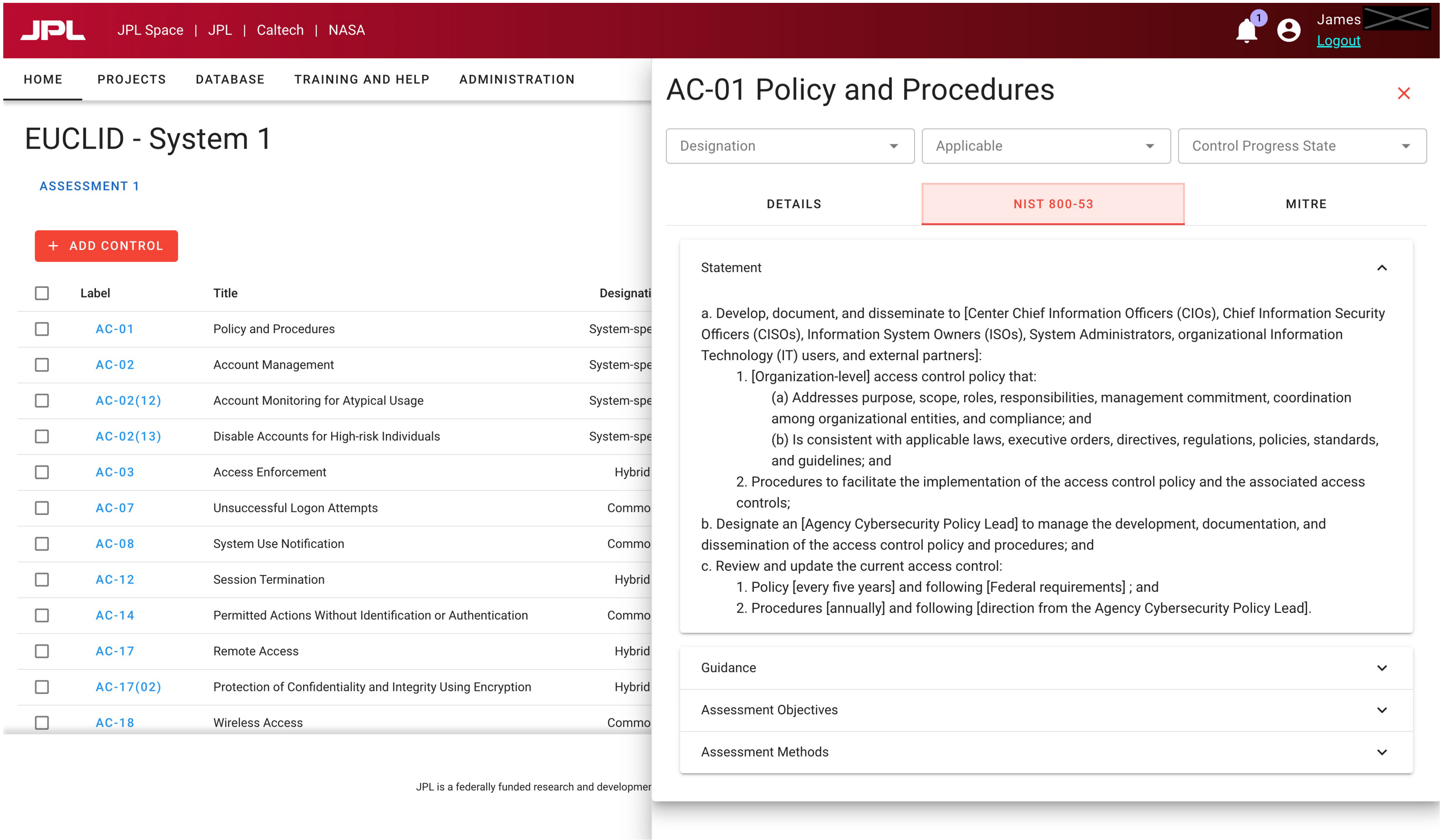
Observations

- Evaluation 1
- Evaluation 2
- Evaluation 3
- Evaluation 4
- Evaluation 5

Commendations

- Evaluation 1

Control Interface – NIST 800-53



JPL Space | JPL | Caltech | NASA

James [redacted]
Logout

HOME PROJECTS DATABASE TRAINING AND HELP ADMINISTRATION

EUCLID - System 1

ASSESSMENT 1

+ ADD CONTROL

□	Label	Title	Designati
□	AC-01	Policy and Procedures	System-spe
□	AC-02	Account Management	System-spe
□	AC-02(12)	Account Monitoring for Atypical Usage	System-spe
□	AC-02(13)	Disable Accounts for High-risk Individuals	System-spe
□	AC-03	Access Enforcement	Hybrid
□	AC-07	Unsuccessful Logon Attempts	Commo
□	AC-08	System Use Notification	Commo
□	AC-12	Session Termination	Hybrid
□	AC-14	Permitted Actions Without Identification or Authentication	Commo
□	AC-17	Remote Access	Hybrid
□	AC-17(02)	Protection of Confidentiality and Integrity Using Encryption	Hybrid
□	AC-18	Wireless Access	Commo

JPL is a federally funded research and developmer

AC-01 Policy and Procedures

Designation ▾ | Applicable ▾ | Control Progress State ▾

DETAILS | NIST 800-53 | MITRE

Statement

a. Develop, document, and disseminate to [Center Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Information System Owners (ISOs), System Administrators, organizational Information Technology (IT) users, and external partners]:

1. [Organization-level] access control policy that:
    (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Agency Cybersecurity Policy Lead] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

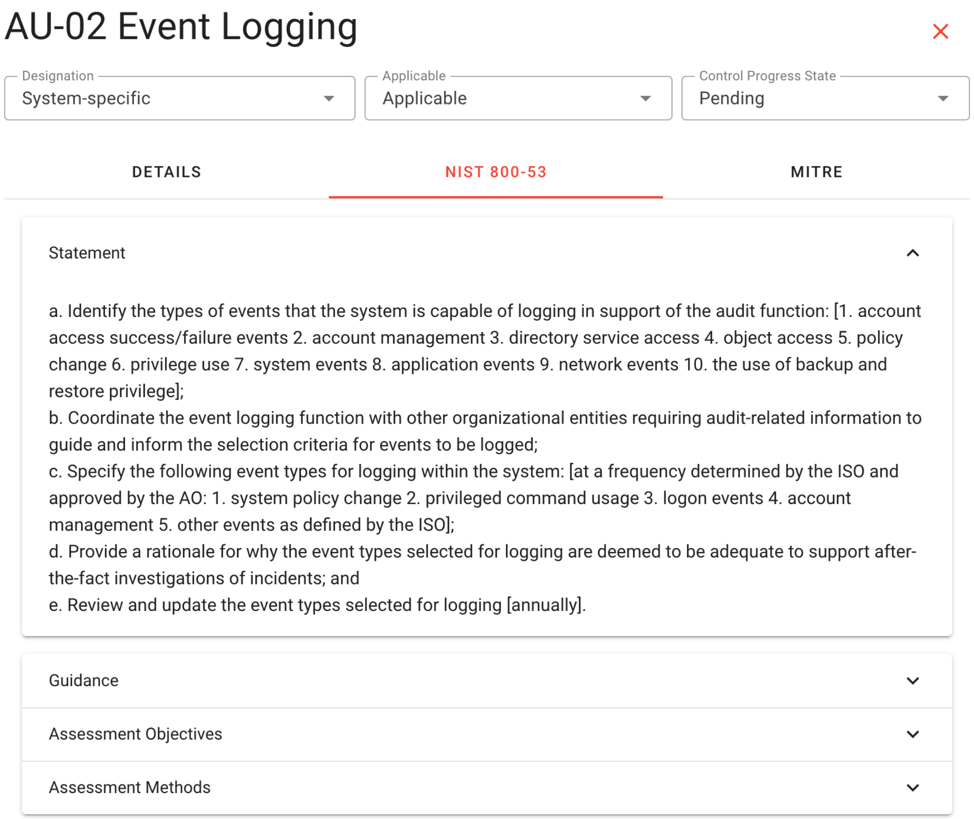
1. Policy [every five years] and following [Federal requirements] ; and
2. Procedures [annually] and following [direction from the Agency Cybersecurity Policy Lead].

Guidance ⌄

Assessment Objectives ⌄

Assessment Methods ⌄

Side-by-Side Comparison

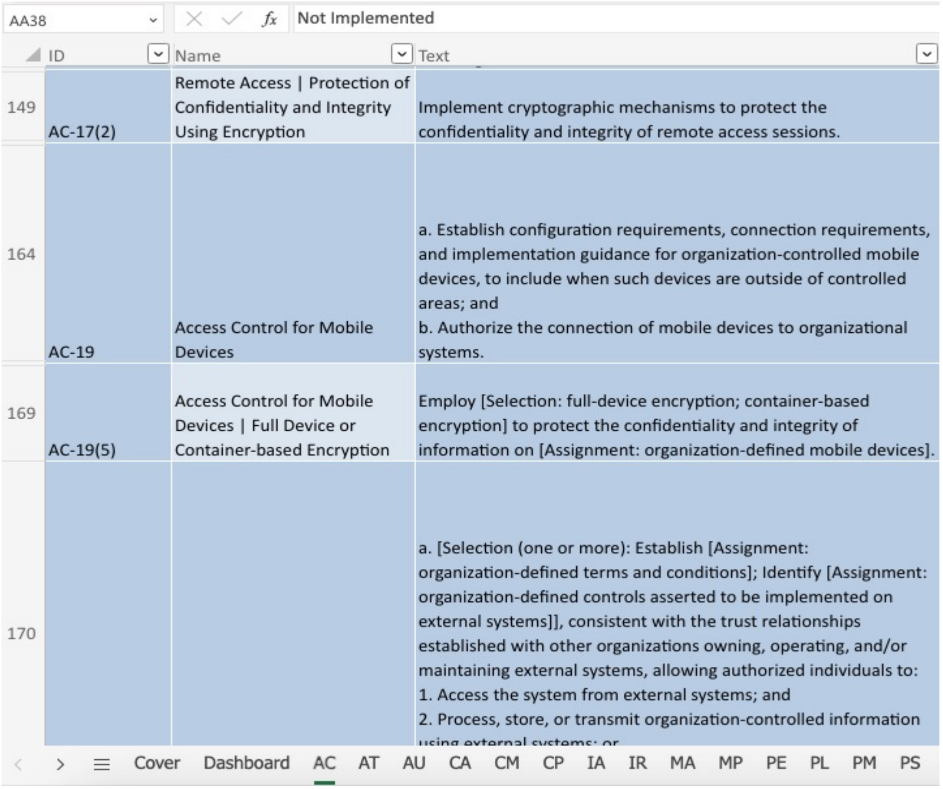


AU-02 Event Logging

Designation: System-specific	Applicable: Applicable	Control Progress State: Pending

Statement

a. Identify the types of events that the system is capable of logging in support of the audit function: [1. account access success/failure events 2. account management 3. directory service access 4. object access 5. policy change 6. privilege use 7. system events 8. application events 9. network events 10. the use of backup and restore privilege];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [at a frequency determined by the ISO and approved by the AO: 1. system policy change 2. privileged command usage 3. logon events 4. account management 5. other events as defined by the ISO];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [annually].



AA38 | Not Implemented

	ID	Name	Text
149	AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
164	AC-19	Access Control for Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.
169	AC-19(5)	Access Control for Mobile Devices | Full Device or Container-based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].
170			a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or

Future Possibilities

How can further development benefit NASA?

- Help assessors conduct faster assessments
- Onboard new-assessors through a guided introduction on the website
- Improved assessor collaboration

Acknowledgements

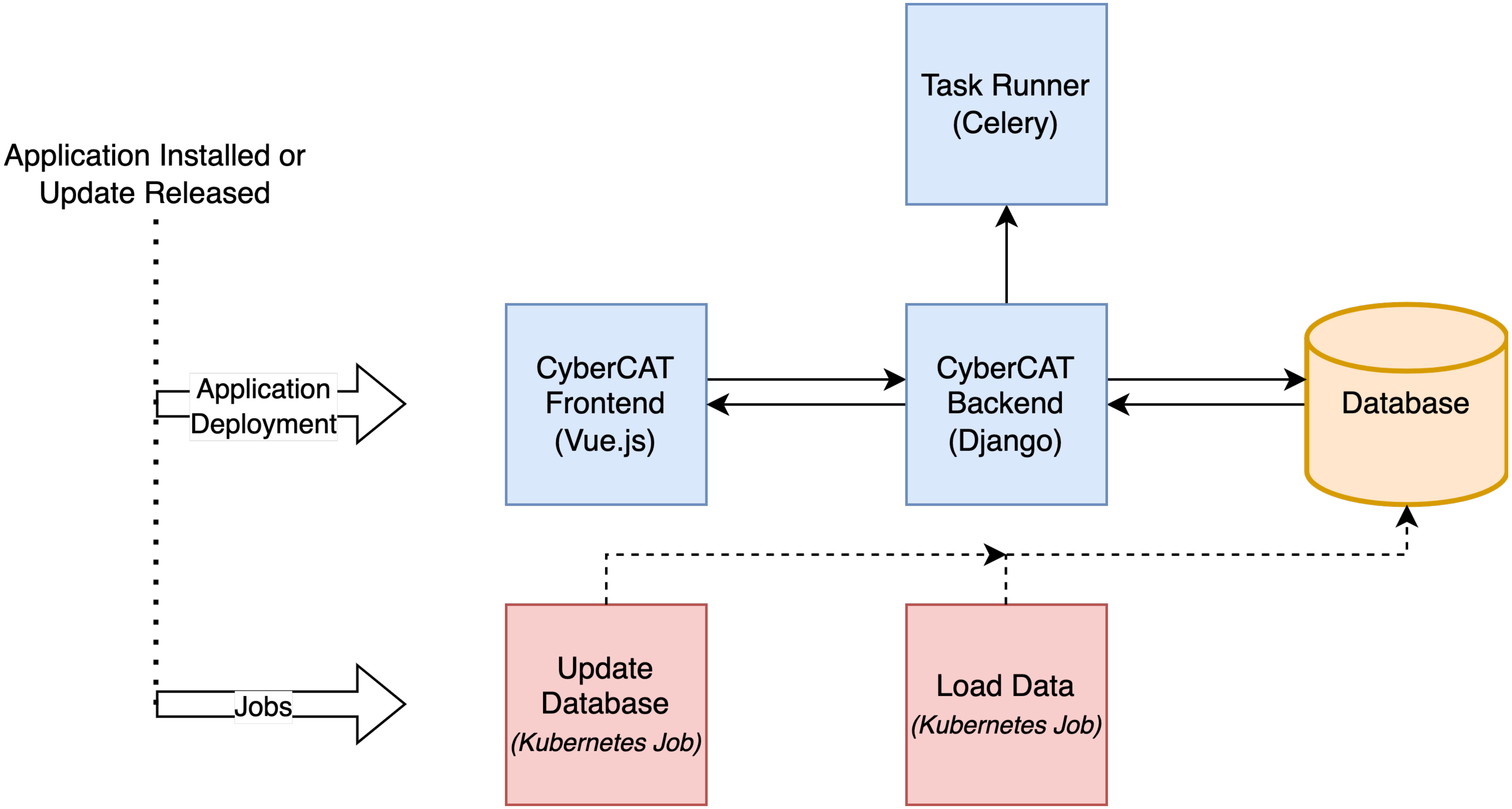
- Cristopher H[redacted]
- Steven [redacted] G[redacted]
- James M[redacted]
- Lyle B[redacted]
- JPL Higher Education Department

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov

Application Architecture

Deployed in Kubernetes


Task Runner (Celery)
Application Installed or Update Released
Application Deployment
CyberCAT Frontend (Vue.js)
CyberCAT Backend (Django)
Database
Jobs
Update Database *(Kubernetes Job)*
Load Data *(Kubernetes Job)*

Acknowledgement Statement

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, and was sponsored by Maximizing Student Potential and the National Aeronautics and Space Administration (80NM0018D0004).