

# **COLERIDGE** INITIATIVE

## SECURITY MODULE

## Contents

1. Motivation .....	3
2. Context .....	3
3. Current Approach .....	3
3.1 Safe Setting .....	4
3.2 Safe People .....	5
3.3 Safe Projects .....	7
3.4 Safe Data .....	9
3.5 Safe Output .....	10
4. The Future .....	12
4.1 Example of Customizations .....	12

## 1. Motivation

System security protocols are essential to keep and share sensitive data between members. The ADRF's security module is designed to address such needs for the sharing of restricted administrative data. This document provides the following:

- (i) a summary of the existing ADRF approach,
- (ii) a discussion of how this approach might be customized and built upon.

## 2. Context

Data security in the ADRF is built on a cloud-based system that provides secure access to restricted administrative data. The ADRF security module ensures that data security and confidentiality are enforced on five different levels: (i) at the level of safe settings or infrastructure; (ii) at the level of safe people, making sure only authorized users have access to the system; (iii) at the level of safe projects in access-controlled workspaces and services which ADRF users can make use of in their work; and at the level of (iv) safe incoming data as well as (v) safe data outputs through extensive review by system administrators and data stewards.

This document provides further details of the implementation at each level in the particular context of the United States Federal Risk and Authorization Program (FedRAMP), a US government-wide program for assessing, authorizing, and standardizing security in cloud-based products and services.<sup>1</sup>

## 3. Current Approach

The ADRF's approach to security is informed by the Five Safes framework, first developed by Felix Ritchie at the UK Office for National Statistics (ONS).<sup>2</sup> **Figure 1** summarizes how ADRF infrastructure, users, staff, and services that control system access and usage map to the Five Safes to protect restricted administrative data stored in the ADRF and guards against unauthorized disclosure of that data. Below details how the ADRF Secure Border, implementation of standard security protocols, and infrastructure constitutes **Safe Settings**, how the careful review, management, and tracking of users in the ADRF system ensures only **Safe People** may access and work with data in the ADRF, how the review of project proposals

---

<sup>1</sup> <https://www.fedramp.gov/about-us/about/>

<sup>2</sup> Desai, Tanvi, Ritchie, Felix and Welpton, Richard, (2016), Five Safes: designing data access for research, Working Papers, Department of Accounting, Economics and Finance, Bristol Business School, University of the West of England, Bristol.

by ADRF staff and subsequent user interaction occurring only through secure and access-controlled project workspaces are the basis for **Safe Projects**, and finally how **Safe Data** and **Safe Outputs** are ensured through extensive import and export review processes conducted by data providers and ADRF staff carefully guiding restricted data into and out of a secure, cloud-based data research facility.

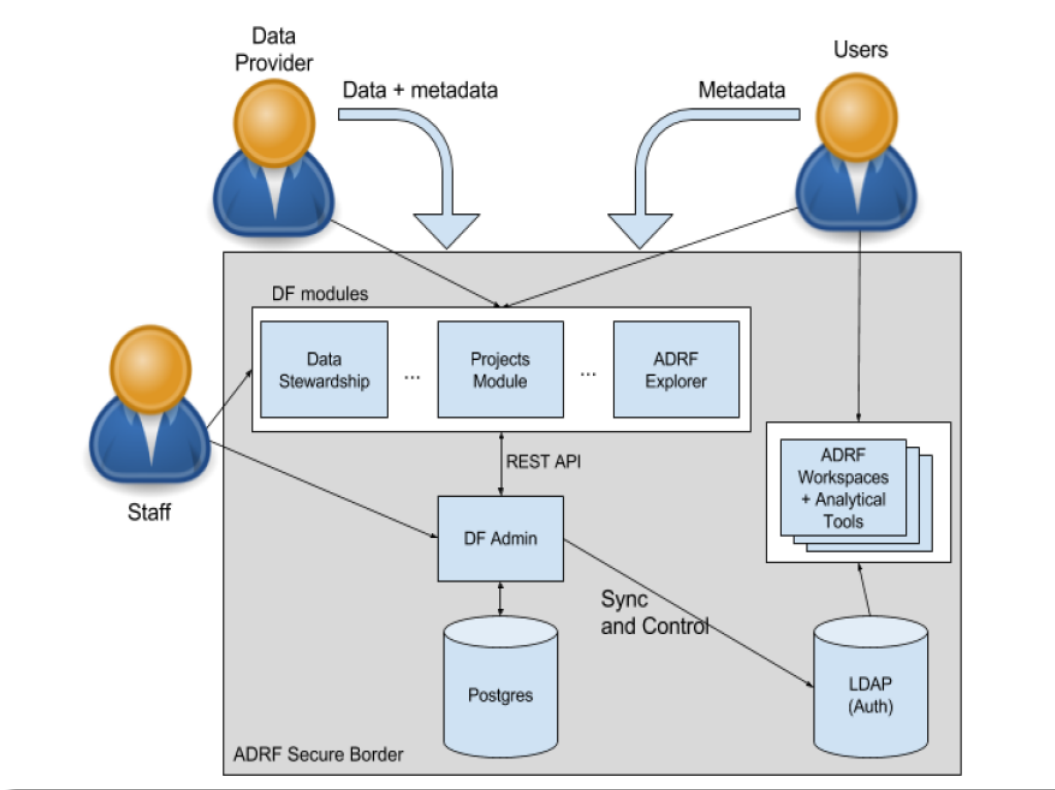


FIGURE 1: OVERVIEW OF ADRF SECURITY

### 3.1 Safe Setting

The foundation for a computing environment which protects the storage, sharing, and analysis of restricted administrative data is a well-designed security infrastructure developed with well-documented security considerations and practices in mind. The ADRF system is currently built inside of the Amazon Web Services GovCloud, which is an isolated AWS region, subject to FedRamp compliance, that allows customers to host sensitive Controlled Unclassified Information (CUI) and regulated workloads.<sup>3</sup>

AWS-provided security features include: (i) Managed DDoS Protection through AWS Shield, a service that provides always-on detection and automatic inline mitigations that minimize downtime and latency; (ii) Secure Access via customer access points, also called Application

<sup>3</sup> <https://aws.amazon.com/govcloud-us/>

Programming Interface (API) endpoints, which allow secure HTTP access (HTTPS) so that customers can establish secure communication sessions using the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols; (iii) Built-In Firewalls giving ADRF administrators the ability to control how accessible its instances are by configuring firewall rules; (iv) Option to use granular user access rules through the AWS Identity and Access Management (IAM) tool that permits administrators to control the level of access users have to AWS infrastructure services; and finally (v) Multi-Factor Authentication (MFA) to reinforce security of user logins through a single use access code generated anew at each login.

The ADRF has completed a FedRAMP Authorization package including the required System Security Plan (SSP), Incident Response Plan (IRP), Configuration Management Plan (CMP) as well as all other required documentation. The Technical, Management and Operational controls were documented by Earthling Security.<sup>4</sup> A successful FedRAMP Readiness Assessment has been completed by an accredited Third Party Assessment Organization (3PAO). A complete FedRAMP Continuous Monitoring program is implemented and has been reviewed by the FedRAMP 3PAO as part of the Readiness Assessment.

After reviewing our completed FedRAMP pre-Readiness Assessment, the Census Bureau has provided the ADRF system with an Authority to Test. As such, we have moved to the next step towards Provisional and then full FedRAMP approval. The ADRF FedRAMP security procedures are documented in a 400-page system security plan submitted to the Census.

## 3.2 Safe People

ADRF administrative staff and data stewards manage and track user access and usage of datasets as a necessary component of a secure computing environment. User management in the ADRF Security module functions by: (i) requesting that users apply for and verify their identities before gaining access to protected administrative data; (ii) mandating that users read and agree to data usage agreements defining acceptable usage of datasets in the ADRF and ramifications for violating or ignoring those usage requirements; (iii) assigning users unique system identities in order to access the system; and (iv) providing administrators tools like the Data Facility Administrator (DF Admin) to track and manage user access to data based on whether each user has satisfied all necessary requirements to access certain datasets as per their terms of use or data usage agreements.

### **Review and Acceptance of Users**

At the center of safe people in the ADRF is review of users before they are provided access to the system. Currently, user review revolves around the Applied Data Analytics (ADA) course currently being run on the ADRF. In order to be considered for the course, potential users must be current employees of a government entity and submit a resume, a statement of purpose,

---

<sup>4</sup> <http://www.earthlingsecurity.com/>

and a letter of support from the entity with whom they work. This submission process serves two purposes: (i) it is to verify the individual as an employee of a government entity and (ii) it is to affirm that the intended purpose of the individual in gaining access to data in the ADRF via the ADA course is appropriate based on the terms of use for the datasets to be used in the course. If users are accepted, they are then required to read, agree to, and sign data use agreements and an agreement for usage of the ADRF which outlines the care they must observe in accessing the data and what they can and cannot do with the data in the ADRF.

### **DF Admin for Managing User Access**

DF Admin is the open source tool built inside of the ADRF to control and manage the interaction between all entities inside of the ADRF. DF Admin provides a common place for ADRF administrators to inquire about and control the administrative metadata used to control access to and interactions between the different elements of the ADRF. It is also built to process requests for access, update permissions in the Lightweight Directory Access Protocol (LDAP) system,<sup>5</sup> and provide access to information and core processes via APIs for applications and services in the ADRF. DF Admin tracks defined system entities as well as associated workflows. These entities include (i) users, (ii) projects (including project agreements, source and stewardship contacts, etc.), and (iii) data sets. Example workflows include providing access rights to users for projects and datasets, creating and managing projects with actions such as adding users or data sets to them, and performing necessary steps in the data lifecycle such as ingest, setting access rights to data, disseminating data to the appropriate users, as well as deleting and archiving datasets. **Figure 2** provides a visual overview of the entities captured in DF Admin's data model and the interactions between them, it is simplified for clarity.

---

<sup>5</sup> [https://en.wikipedia.org/wiki/Lightweight\\_Directory\\_Access\\_Protocol](https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol)

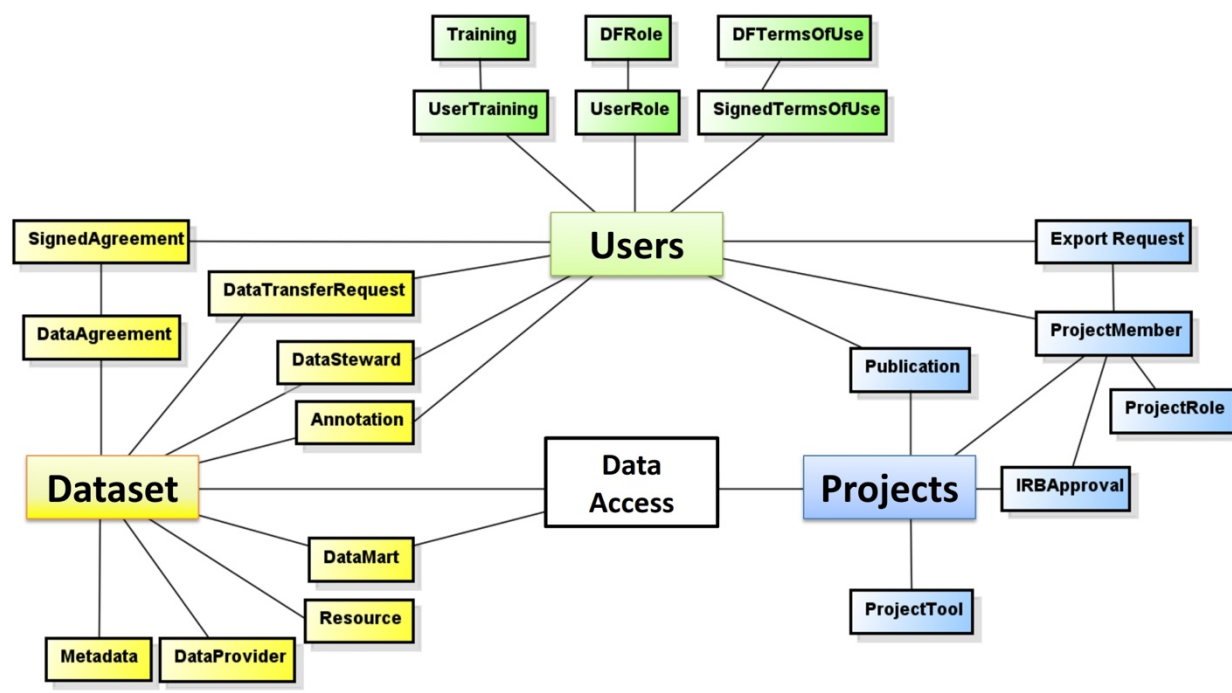


FIGURE 2: DF ADMIN ARCHITECTURE (SIMPLIFIED)

DF Admin is designed as a single centralized management superstructure in order to map to the interleaved nature of the workflows executed daily in the ADRF along with the need to consistently and reliably take the permissions and relationships between entities into account when setting user access rights. Consider, for example, the workflow to grant data access to a project. Processes must be put in place to monitor multiple entities and their relationships – such as which datasets are approved for a project and which individuals are authorized to work on a project. These workflows can be high-level processes (e.g., for ensuring that users with access to data fulfill all required training and sign all required forms before they are provided access to actual data) or system-level processes (e.g., processes that manage membership within an operating system or database group that controls access for other users). The many elements that must be considered when deciding whether a given user can access a given dataset, and the critical nature of managing and tracking these actions, requires a single, centralized, canonical source for this information.

### 3.3 Safe Projects

Projects are the central point at which users and data converge, therefore they are a component where the ADRF Security module is most performant. Safe projects are established by both carefully reviewing and accepting projects and by managing access to projects for ADRF users.

## Project Review

Much like review of users, project safety is aided by a review of projects before allowing them to be created in the ADRF. For the ADA course, the prospective participants submit a statement of purpose with their application to be included in the course. This statement of purpose includes a detailed description of the project they would like to work on inside of the ADRF as a major part of their coursework. At this point, potential projects are reviewed for their appropriateness to the data existing in the ADRF. For example, a project which seeks to predict chances of a population returning to jail based on several aspects of their involvement in public assistance services would be an appropriate project for inclusion in the ADRF. On the other hand, a project which seeks to identify individuals involved in public assistance fraud based on a set of offenses and history of employment would not be a permissible project in the ADRF. That is, review of projects in the ADRF serves to avoid creating projects or conducting analyses in the ADRF which could potentially disclose specific information about individuals in any way.

## Identity and Access Management

Access to different ADRF functions or datasets stored within the ADRF is centered on user access to projects which in turn is determined by an individual's role (e.g., system administrator or end-user) and further broken down by role groups (e.g., administrative users who are authorized to perform installation of new software in the ADRF or members of a specific project). This design allows the ADRF to comply with the Access Controls defined by FedRAMP while flexibly organizing individuals into projects which, once approved by the necessary parties (such as data providers), provides access to approved datasets.

Identity and rights within the ADRF environment are maintained by OpenLDAP<sup>6</sup> and WSO2.<sup>7</sup> Keycloak<sup>8</sup> adds two-factor authentication to the ADRF platform and integrates with the OpenLDAP structure to provide a single point of truth for system access and data control. All services in the ADRF which require a user login will first query Keycloak to authenticate user access rights. There are two different types of roles within this module: *static* and *dynamic*.

*Static* groups are set roles based on how the individual user is allowed to interact with the ADRF and allows for various subsets of users' access to be controlled *en masse*. For example, any user that is part of the "annotation-reviewers" group has access to moderate which user comments are approved for display in the ADRF Explorer.

*Dynamic* groups determine access to which project(s), dataset(s), and database(s) users have access within the ADRF and are dynamic because these access rights can change overtime. An example of this is class dataset access in the Applied Data Analytics (ADA) training program. Each class has access to some of the same datasets and one distinct dataset each. To ensure both classes did not have access to data they were not supposed to within the space used for

---

<sup>6</sup> <https://www.openldap.org/>

<sup>7</sup> <http://wso2.com/>

<sup>8</sup> <http://www.keycloak.org/>



the training materials, different groups are created for each new class (or cohort of participants) in order to isolate class specific datasets only to the correct group of participants who should have access to them (based on agreeing to specific terms of usage for each dataset and the review process by ADA staff determining who can take the course in the first place). Once the class is over, administrators can set user access in that class to expire. Similarly, data usage agreements for a specific dataset may specify that user access to a dataset expires after a stated period of time.

### 3.4 Safe Data

ADRF staff make sure that the data coming in are safe by (i) establishing rules and policies in data usage agreements with official data providers, (ii) securely transferring data from data providers to ADRF staff using end-to-end encryption, (iii) reviewing, cleaning, and de-identifying or hashing Personally Identifiable Information (PII) in the dataset, and (iii) safely and securely ingesting and storing data into the ADRF.

#### **Data Acquisition and Agreements**

Determining which data to include, how much of it, and what terms of use go along with that data in the ADRF is an essential first step in first bringing data into the ADRF and ensuring that its inclusion would not create a disclosure risk. As datasets are identified for a class, it is necessary to confirm that everything transferred to the ADRF will be permissible. This is critical because if students or other users are not approved to access any of the data in the datasets accessible to them, this would be a potential violation of the data agreements created cooperatively by ADRF staff and the providers of the original data. The data agreements have to be carefully examined by staff to ensure that datasets or data items are not accessible to ADRF users who do not have a permissible research need.

#### **Secure Transfer, De-identification, and Secure Data Ingest**

As a result of refining the ingest and storage process we have two similar, but distinct, data transfer and storage procedures depending on whether the data is Title 13 from the Census Bureau or confidential micro-data from a different agency. Additionally, we have a third, less restrictive process for transferring publically available or other, non-confidential datasets. Next in this section we outline our general data ingest processes, how data are stored in the ADRF, and the ingest process for the more restrictive Title 13 data.

**General data ingest workflow:** in support of the Applied Data Analytics training program we developed a flexible data ingest workflow for participants from different agencies to ingest their data to the ADRF. At a high level the steps for ingesting confidential data are: (i) a data use agreement is put in place; (ii) the user submits a data transfer request; (iii) the Data Curator, an application administrator for the ADRF, ensures all the required information is submitted and provides secure transfer information to the data provider, (iv) the data provider transfers data

to a secure staging server; (v) if de-identification is required the Data Curator transfers data via encrypted USB to a secure, air-gapped (not connecting to any network of computers nor the Internet) computer and a de-identification process is run based on the contents of the data and the data agreement; (vi) data is run through the ingest scripts we created to standardize the data and metadata format; (vii) data and associated metadata are transferred via secure connection using a VPN and containerized transfer points to the ADRF secure S3 storage on AWS; and (viii) data is indexed to make it discoverable – to those with permission to access it – within the ADRF Explorer. Below are additional details on data transfer, data de-identification, data storage as key elements of the ingest process pertaining to the ADRF security module.

**Transfer encryption:** To ensure that at no point in the transfer process are the data vulnerable to unauthorized disclosure at rest, we instruct all of our data providers to first encrypt their data using the National Institute of Standards and Technology recommendation of an AES 256 cipher<sup>9</sup> and using a public key for which the corresponding private key is stored on a computer which is not attached to the Internet. We then only allow users to transfer data to us using an encrypted connection using the Secure File Transfer Protocol (SFTP). Once it is transferred, we immediately remove the encrypted data and store it on the air-gapped computer where the private key is stored for decrypting.

**De-identification:** We have implemented the policy that any confidential, micro-data ingested to the ADRF will have certain elements (e.g., full names, Social Security Numbers, Business identifiers) de-identified before being made available. As described in the general data ingest workflow above, the de-identification process is run, when necessary, on a secure, air-gapped computer before uploading the data to the ADRF. Given the overall goal of the ADRF – to enable combining confidential data for analysis – we are developing a library of reusable scripts to hash data elements that need to be de-identified so that datasets can later be linked within the ADRF for approved projects. Hashing of variables is done using SHA 256 to ensure that hashed values cannot be cracked.

**Data storage:** We maintain an AWS S3 bucket within the ADRF boundary which is the single point of truth for all data and metadata stored in the ADRF. Unique identifiers for each dataset are used to index datasets for retrieval and, for restricted datasets, determine whether individual users are allowed access. In addition to the S3 bucket, we add heavily used datasets (e.g., those used in instruction materials in the Applied Data Analytics program) to a PostgreSQL database where access is controlled using DF Admin by user groups' privileges based on schemas within the database.

## 3.5 Safe Output

---

<sup>9</sup> <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf>

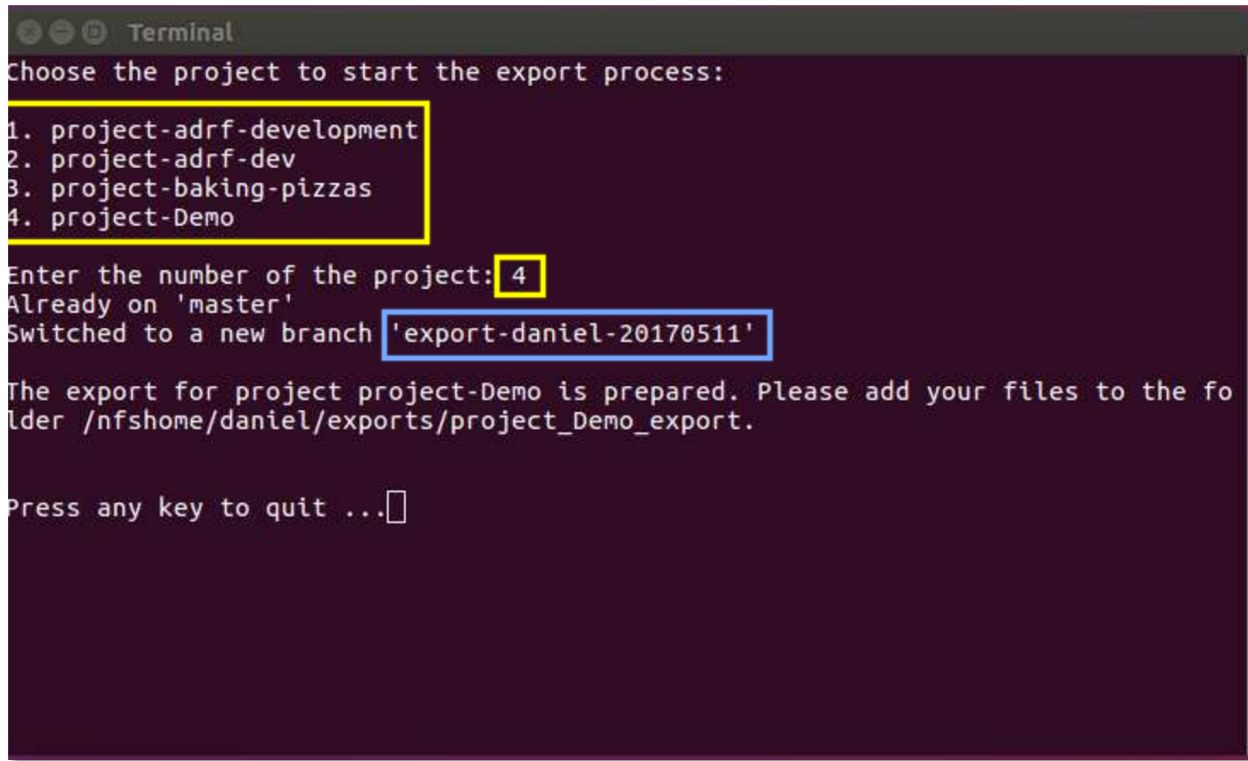
Just as input of data into the ADRF is a tightly controlled and highly supervised process which can only be conducted by specified ADRF administrators, getting data out of the ADRF for purposes of sharing analyses and insights is also tightly controlled and highly supervised. Restricted data are not allowed to leave the ADRF. By system policy, only aggregate numbers, graphs, and other insights and outputs which cannot be used to disclose specific information about individuals represented in the data can be exported from the ADRF. Output export is primarily to serve the purposes of communicating analyses and making policy recommendations. Therefore, there is an extensive review process prior to export of any of these outputs conducted by Data Stewards and data administrators inside the ADRF who are familiar with the handling and risks involved in using data containing PII.

The current export process involves users in the ADRF submitting outputs in an export folder inside the workspace directory for the project they have been authorized to work on inside the ADRF. Users run a Python script which asks them to submit a project from the list of projects they currently have access to (see **Figure 3**). This then initiates a process by which authorized ADRF staff are alerted that a project has been submitted for export and that they must review the contents of the export folder to ensure that no outputs may be used to re-identify users in the data before the outputs may be released to the user for removing from the ADRF.

The ADRF team has worked with different agency partners to define what level of output can be exported and has implemented a set of policies and procedures based on those guidelines and flexible enough for serving different data providers' needs. The guidelines and export request process ensure that policies of both the ADRF and the data providers are met.<sup>10</sup>

---

<sup>10</sup> Full details of the disclosure review guidelines are provided at <https://applieddataanalyticsprogram.org/export-requests> and details of export requests are provided at <https://applieddataanalyticsprogram.org/export-how-to-guide> (password *adrf*).



```

Terminal
Choose the project to start the export process:
1. project-adrf-development
2. project-adrf-dev
3. project-baking-pizzas
4. project-Demo

Enter the number of the project: 4
Already on 'master'
Switched to a new branch 'export-daniel-20170511'

The export for project project-Demo is prepared. Please add your files to the fo
lder /nfshome/daniel/exports/project_Demo_export.

Press any key to quit ...

```

FIGURE 3: TERMINAL INTERFACE TO CURRENT ADRF OUTPUT EXPORT REQUEST

## 4. The Future

While the ADRF Security module provides a full framework of infrastructure, tools, governance, and policy, meeting different needs with the ADRF Security module would still require a better understanding of the specific legal requirements surrounding the sharing of restricted data between organizations.

### 4.1 Example of Customizations

Overall, we see the following customizations necessary for developing the Data Security module:

1. Determine what legal and data governance requirements participating members have in their respective organizations and evaluate what changes must be made to ADRF Security module tools and protocols based on those differences.
2. Better understand the various modules and configurations needed as to how the security module would need to be implemented.

3. Determine the governance structure to determine who would have which responsibilities in managing and administrating security software and for ensuring that members follow security protocols that meet requirements for security compliance.