(1)

Office of the Secretary of Defense (OSD)
Chief Information Officer (CIO)

Joint Information Environment (JIE)

Implementation Plan

Version 1.2

February 3, 2014

SC 4564

Revision History

Version	Date	Description	Revised By
1.0	12/20/2013	Initial Draft Document	David Pham
1.1	1/27/2014	Updated to include data from EITSD, PFPA and OSD Components.	David Pham
1.2	2/3/2014	Updated with additional input from Components.	David Pham

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide a high-level implementation plan for the OSD CIO Joint Information Environment activities in response to the DoD CIO Memorandum "Component Joint Information Environment Implementation Plans," dated November 22, 2013.

OSD CIO developed this implementation plan with input from Washington Headquarters Services (WHS) Enterprise Information Technology Services Directorate (hereby referred to as EITSD), the Pentagon Force Protection Agency (PFPA) and OSD Component Headquarters (hereby referred to as OSD Components).

1.2 Background

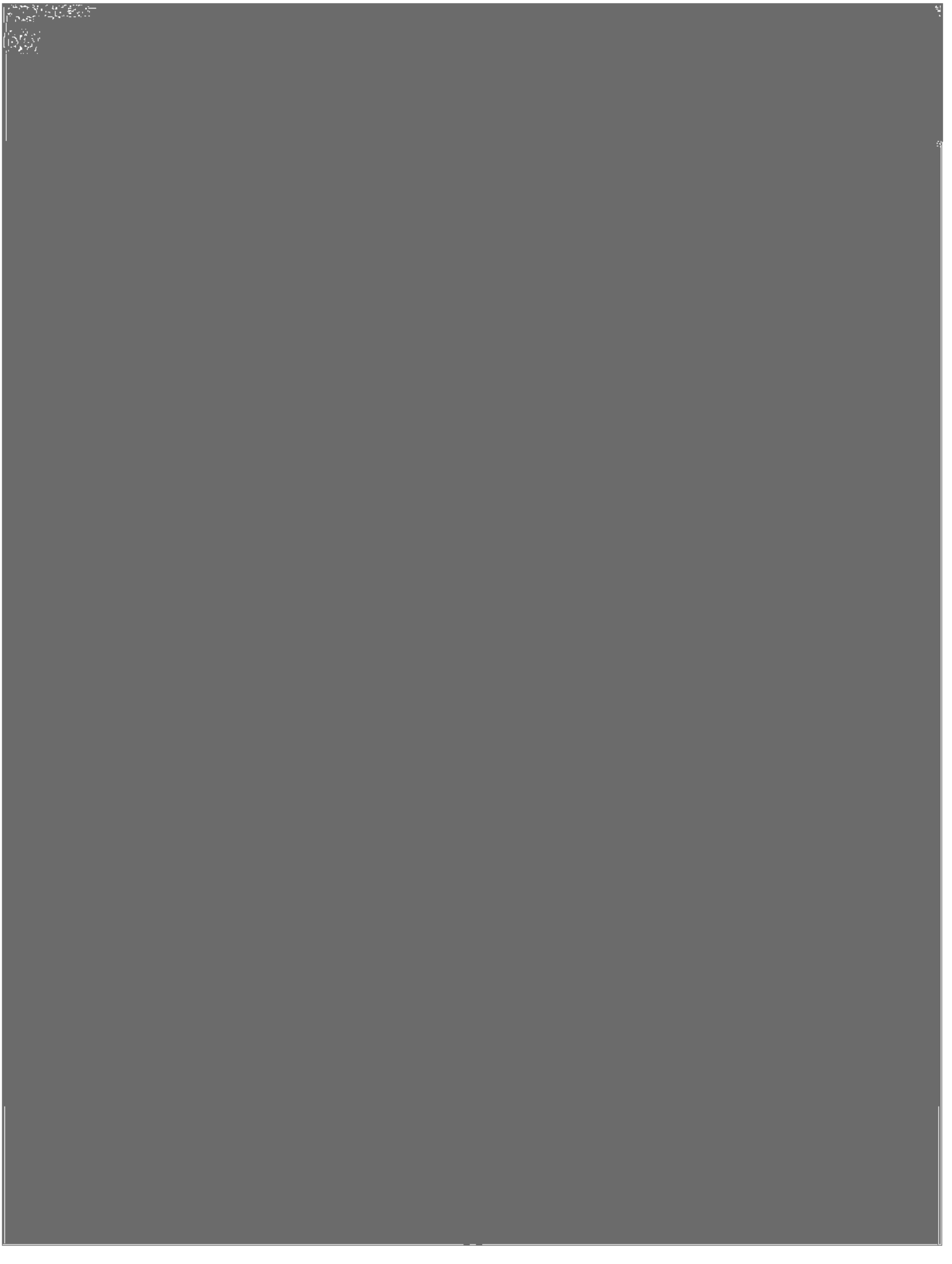
JIE is a secure environment, comprised of shared information technology (IT) infrastructure, enterprise services, and single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE is operated and managed per Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs).

EITSD provides a full range of information technology products, services, solutions and customer support to the OSD Components, the Director of Administration and Management (DA&M), WHS and PFPA to meet mission and business requirements. Specifically, EITSD provides the following services: Collaboration, Identity Protection and Management, Information Security Training and Education Programs, Information Systems Certification and Accreditation/Risk Management, Privacy Impact Assessments, Security Assessments, Telecommunications, Video Teleconferencing and Workstation Support.

1.3 Scope

The scope of this document is specific to services provided by EITSD for the NIPRNET and SIPRNET environments. Additionally, it includes services provided by PFPA and some OSD Component Headquarters for their organization's business systems. It does not include services provided by the OSD Component Field Activities.

(b)(5)



2 JIE Activities

2.1 Network Consolidation

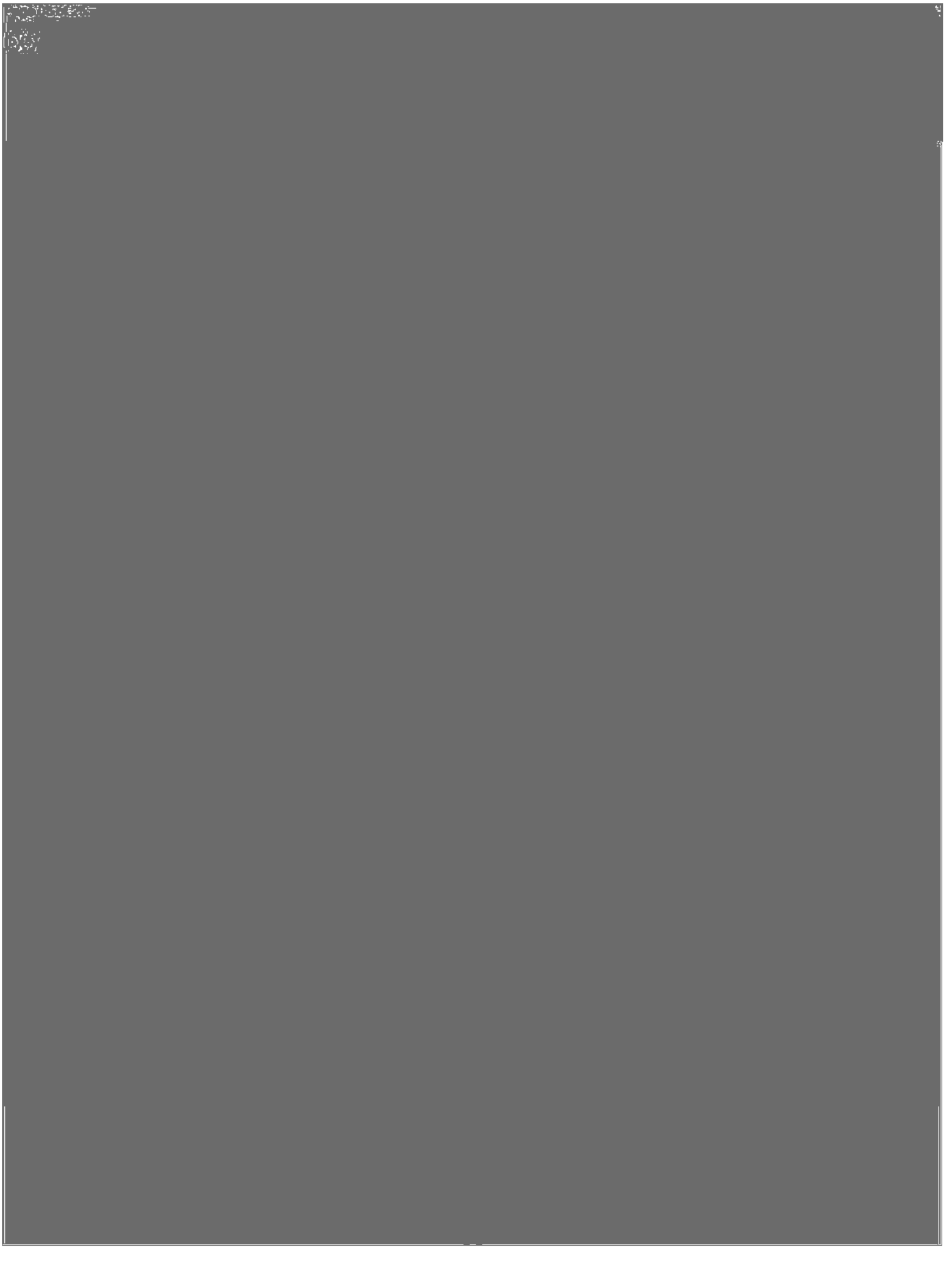
EITSD networks are managed by the US Army ITA. There is no action required.

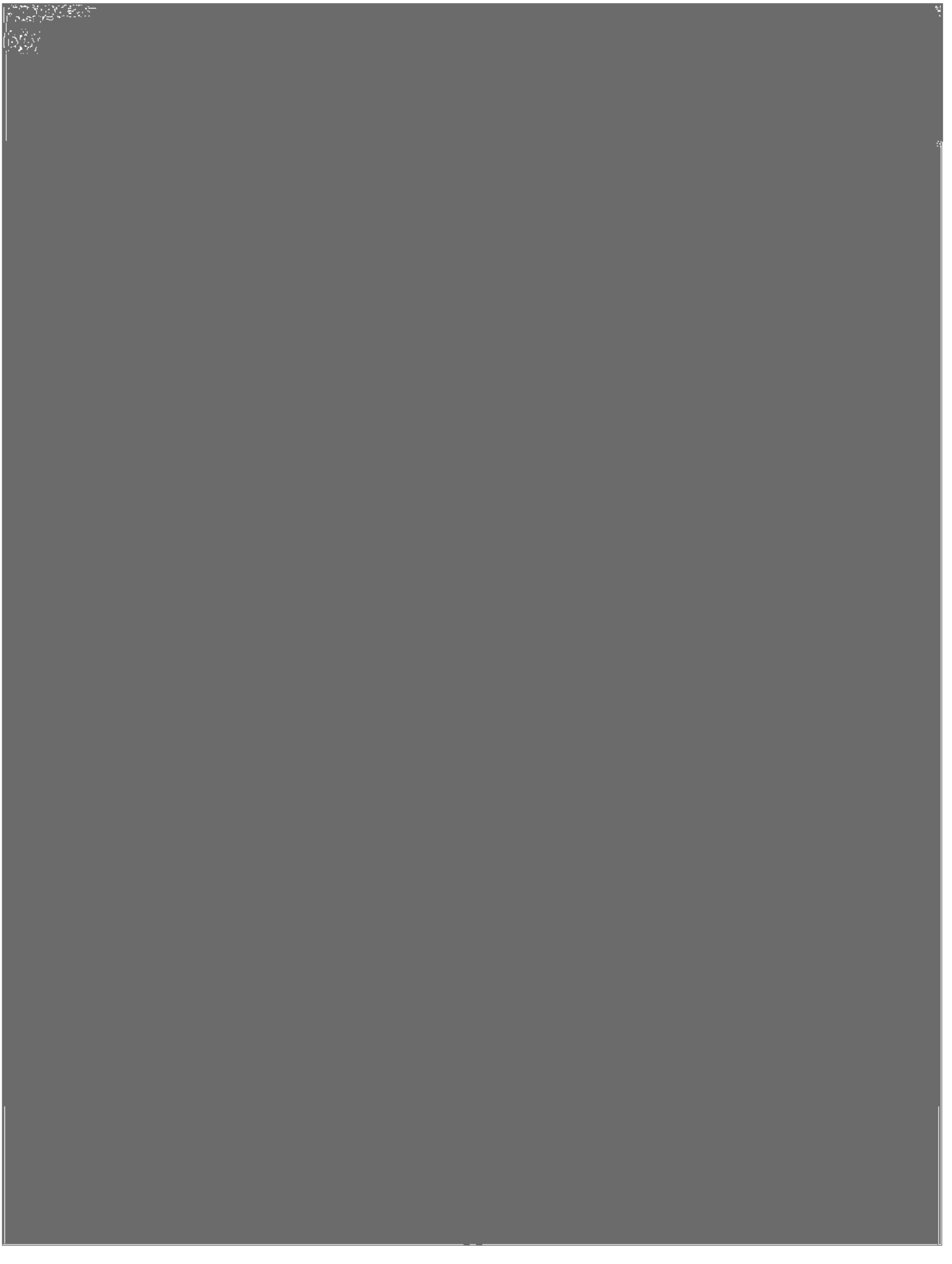
2.2 Internet Facing Applications

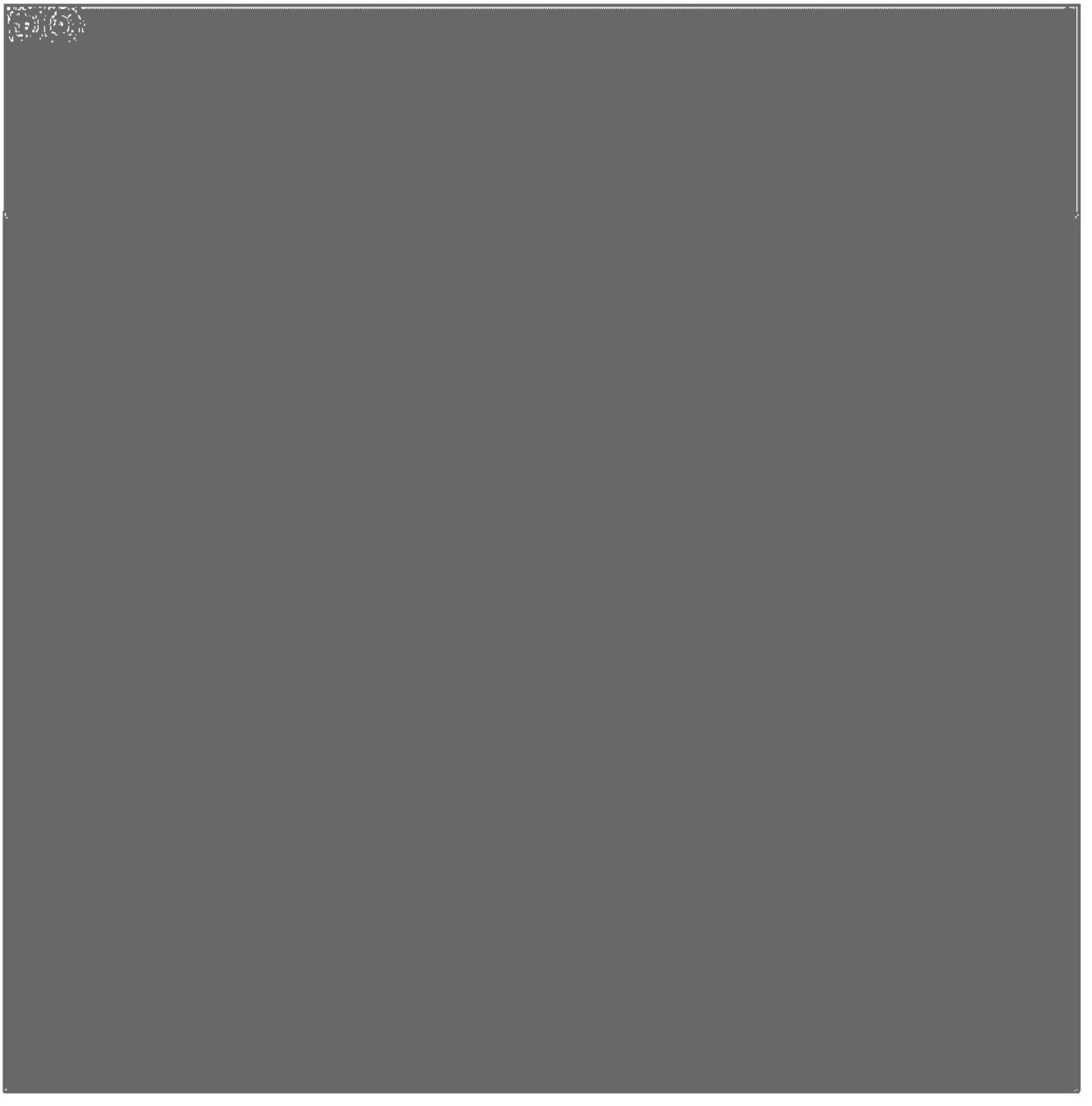
EITSD initiated a pilot in FY 13 to migrate four Internet Facing systems to the DISA DMZ, which is scheduled to be completed in 3rd quarter FY 14. Once completed, EITSD will work with other Components to develop a plan to migrate all Internet Facing systems to the DISA DMZ or Pentagon DMZ. As a result, these systems will not be migrated by the 3rd Quarter FY 14 as directed.

Since the completion date for the Pentagon DoD STIG-Compliant DMZ is unknown, this plan assumes that the Pentagon DMZ will be completed by 4th Quarter FY 2015. The alternative is for these systems to be migrated to other DoD STIG-Compliant DMZs.

The following systems are to be migrated to the Pentagon DoD STIG-Compliant DMZ and to be hosted in the Pentagon IPN:





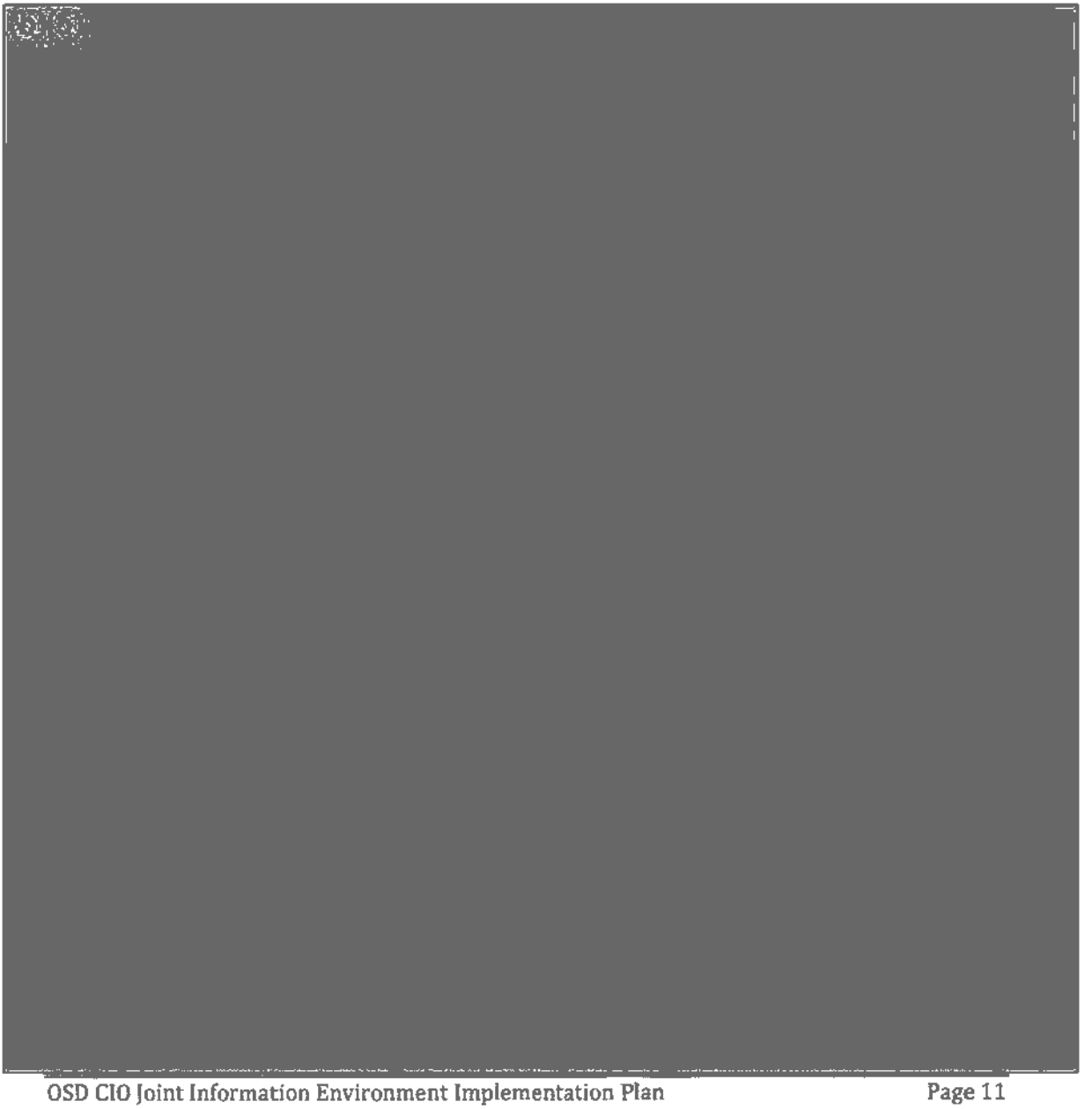


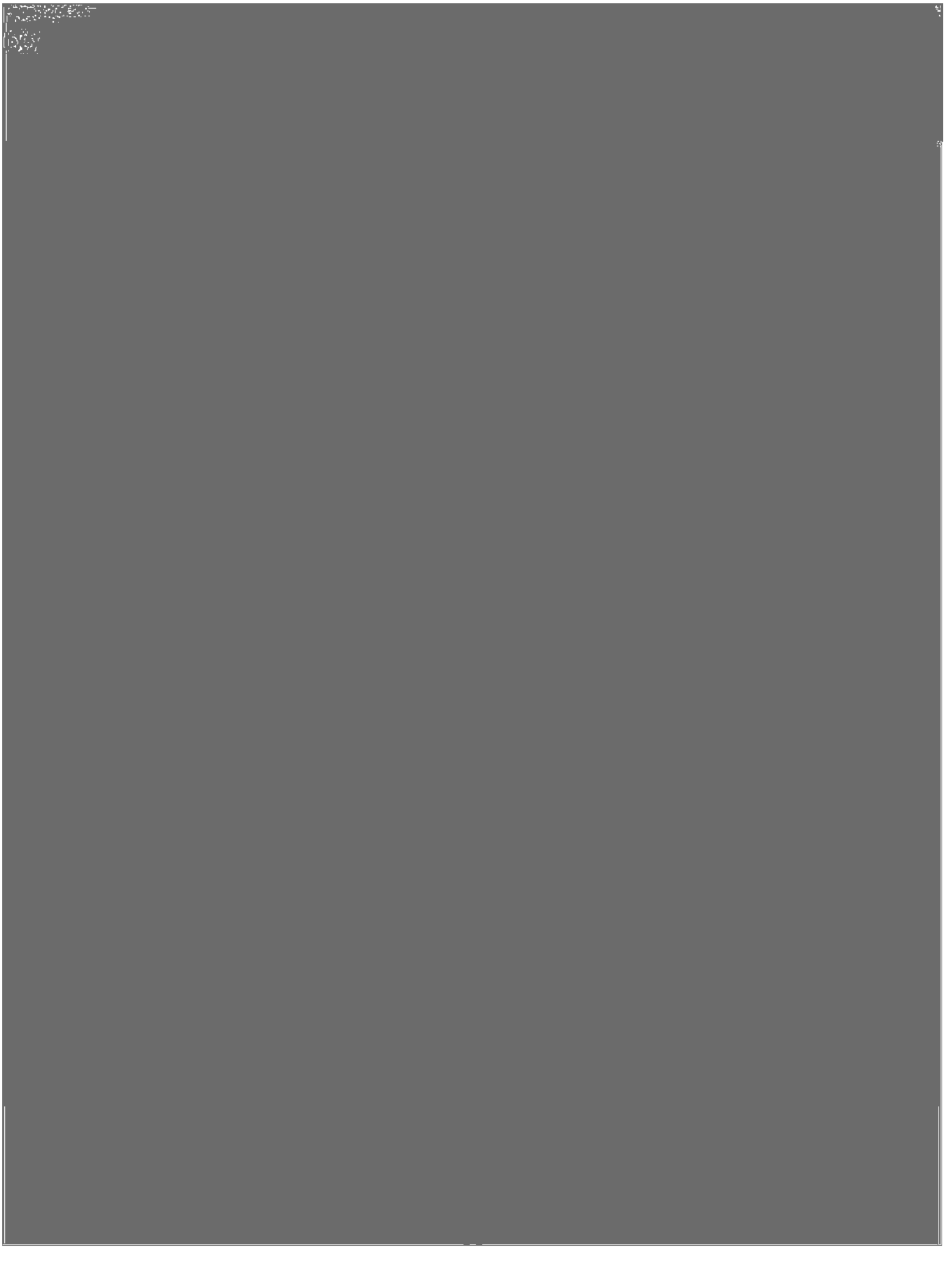
2.4 Enterprise Services: EDS

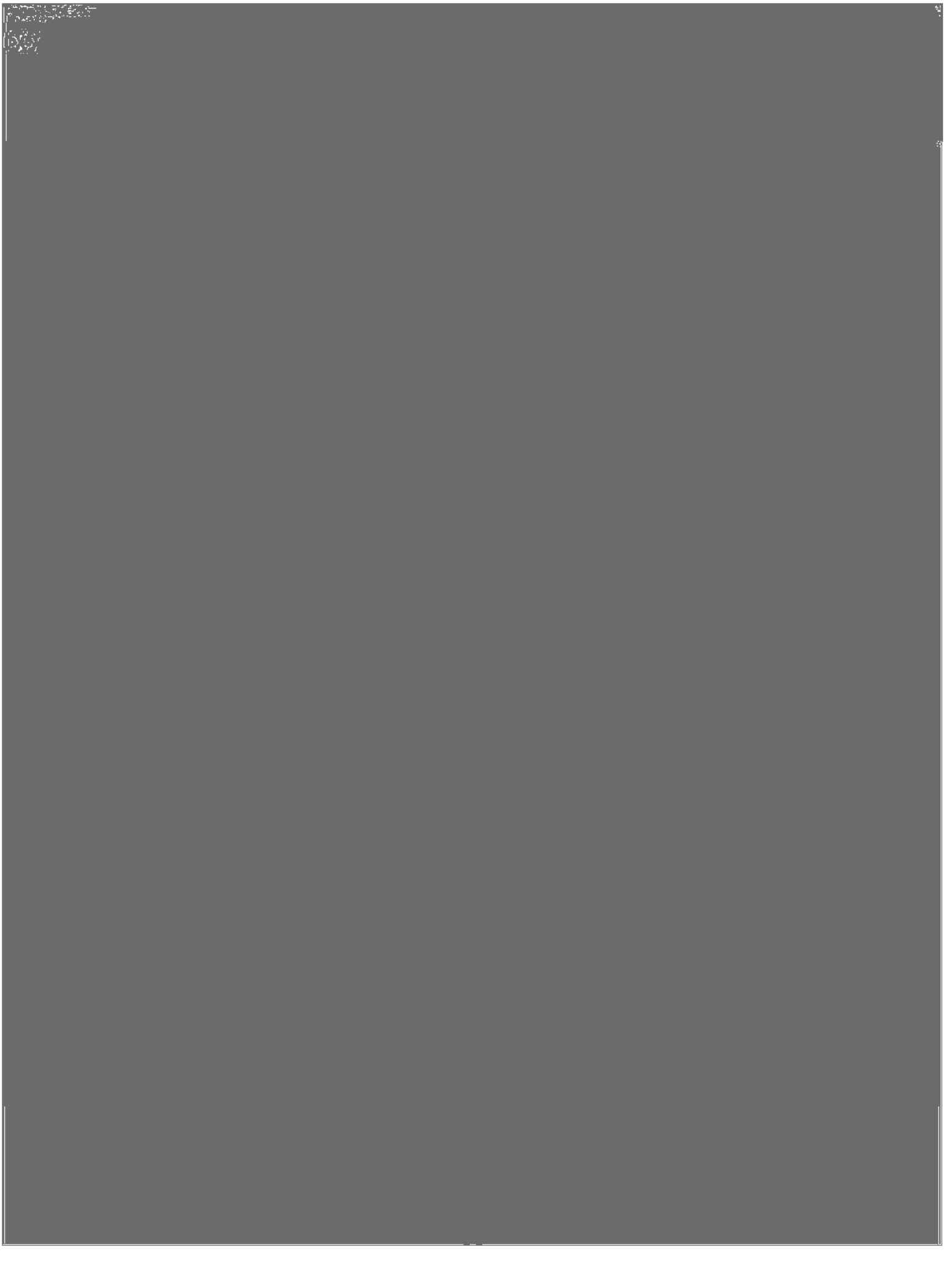
In 2012, EITSD completed a study of existing single sign-on solutions (SSO) and identified that CAPE and AT&L's solutions be served as SIPR and NIPR enterprise SSO, respectively. Furthermore, EITSD worked with CAPE to complete a project to utilize DISA Identity

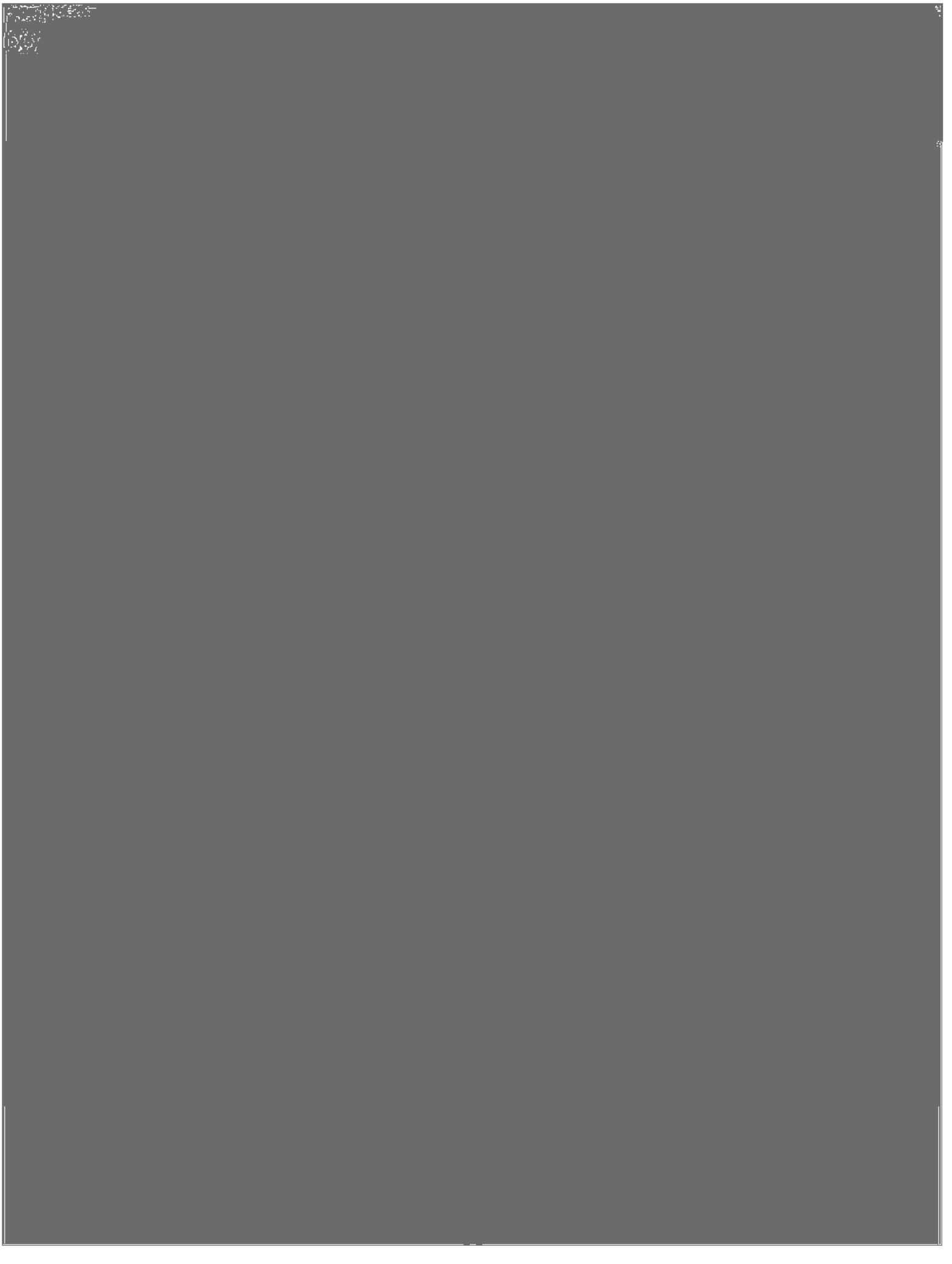
Synchronization Service (IdSS) to authenticate CAPE's SIPRNET applications. In 2013, EITSD worked with AT&L to complete a project to use DISA IdSS to authenticate AT&L's NIPRNET applications.

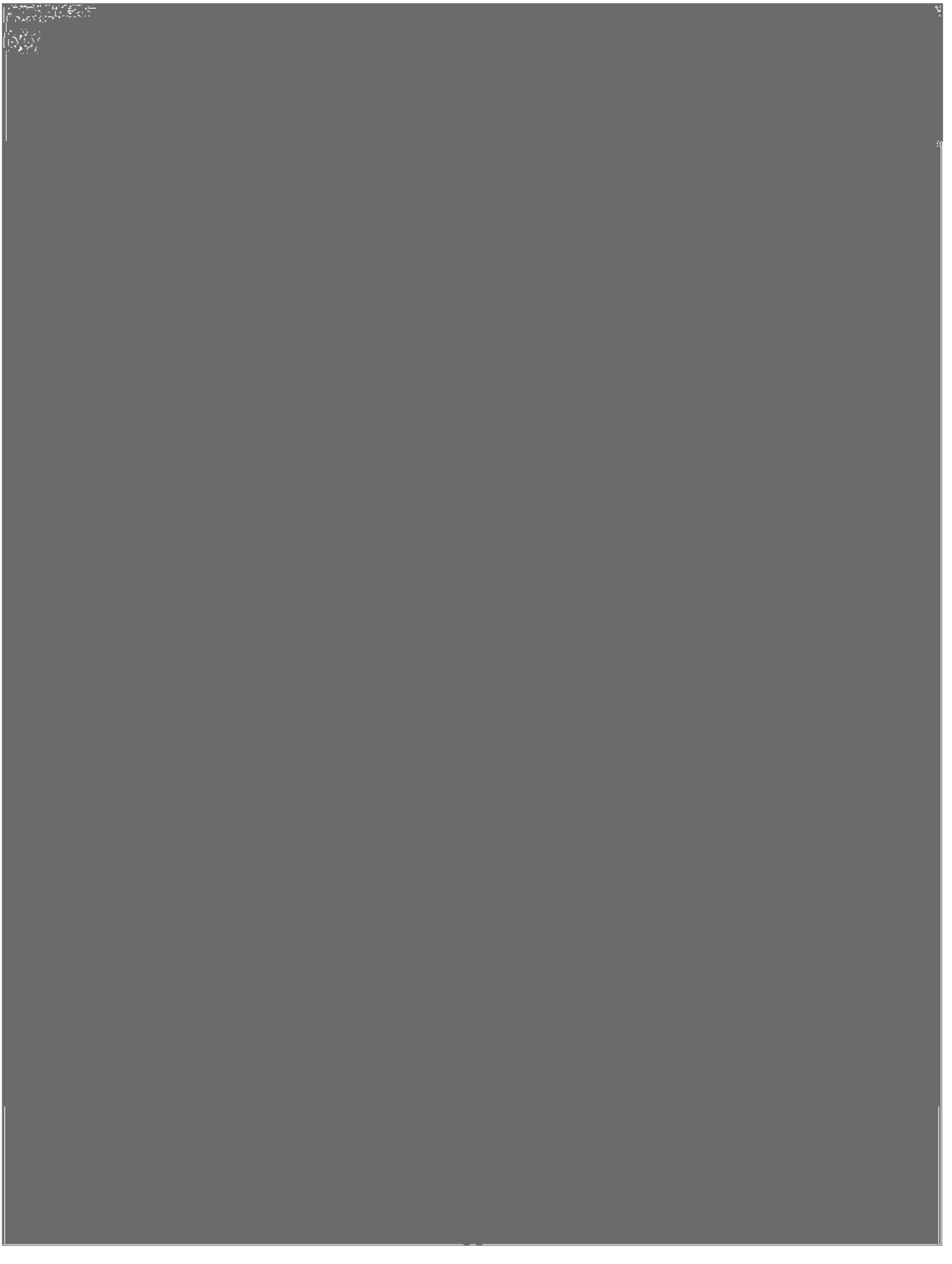
In 2014, EITSD initiated an effort to identify an approach to achieve DoD CIO guidance to PK-enable NIPR and SIPR applications using DISA IdSS. Once completed, EITSD will work with PFPA and OSD Components to develop a project with timeline to achieve DoD CIO guidance. As a result, these systems will not meet the 1st Quarter FY 16 date as directed.

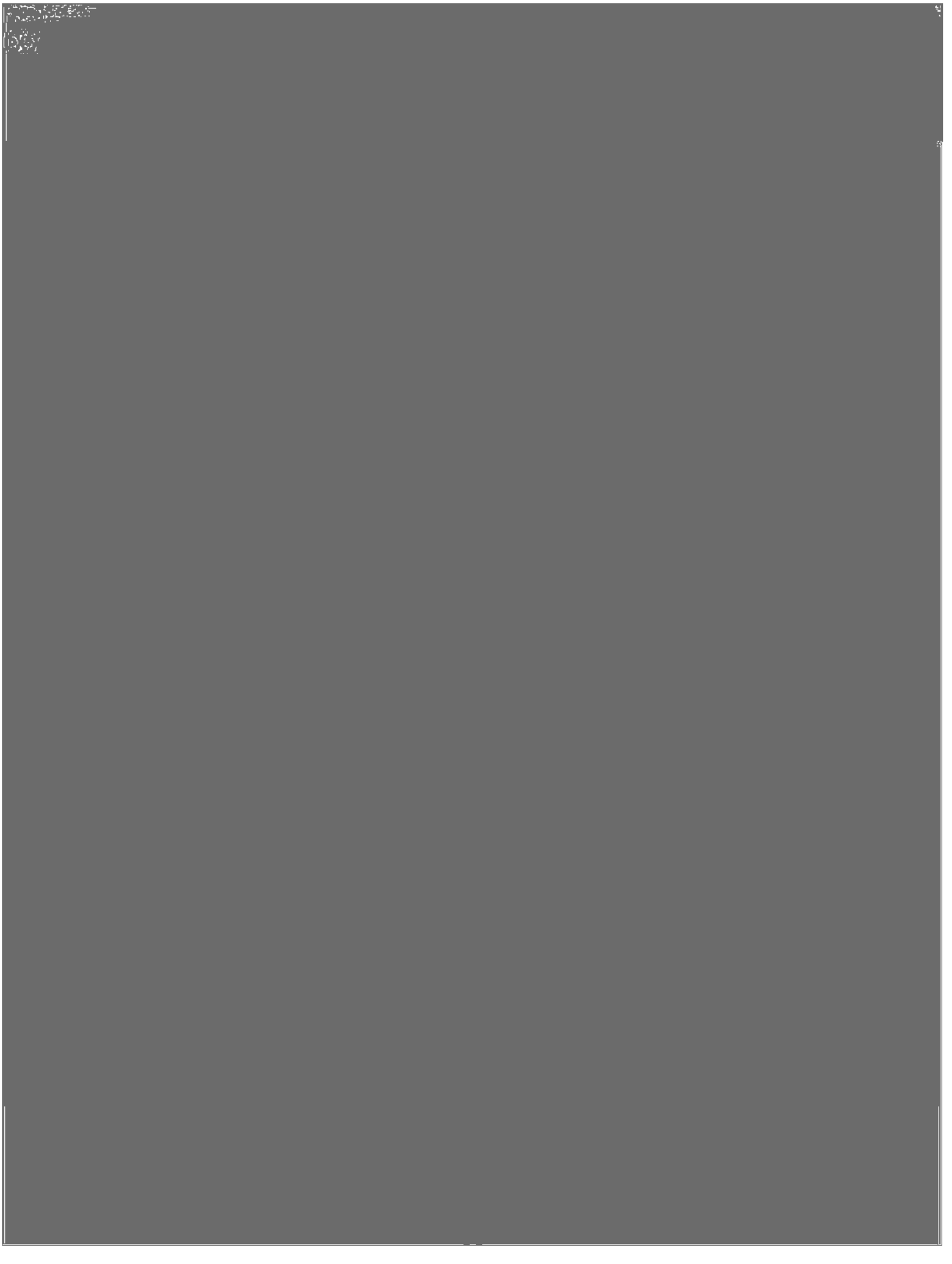


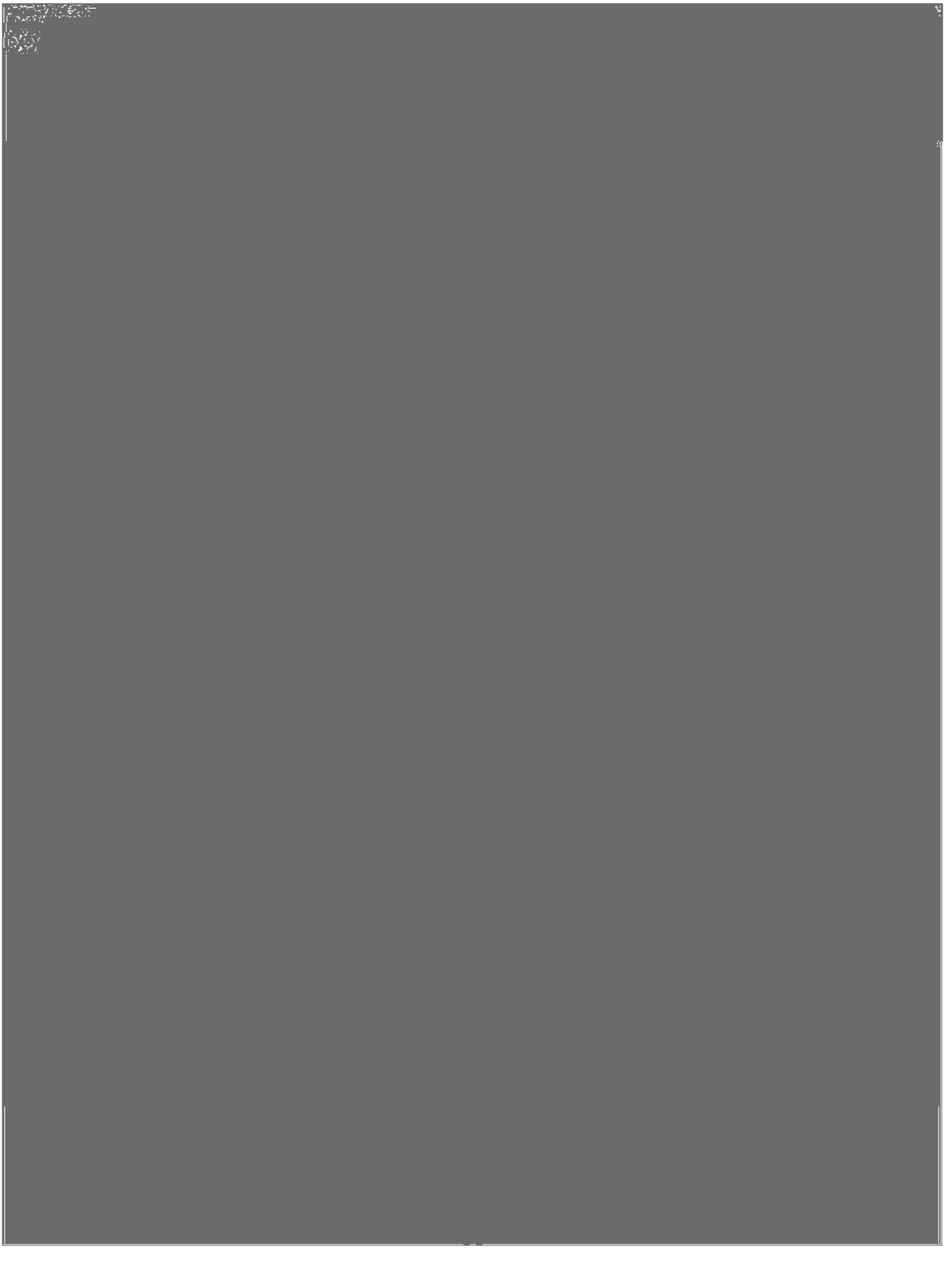






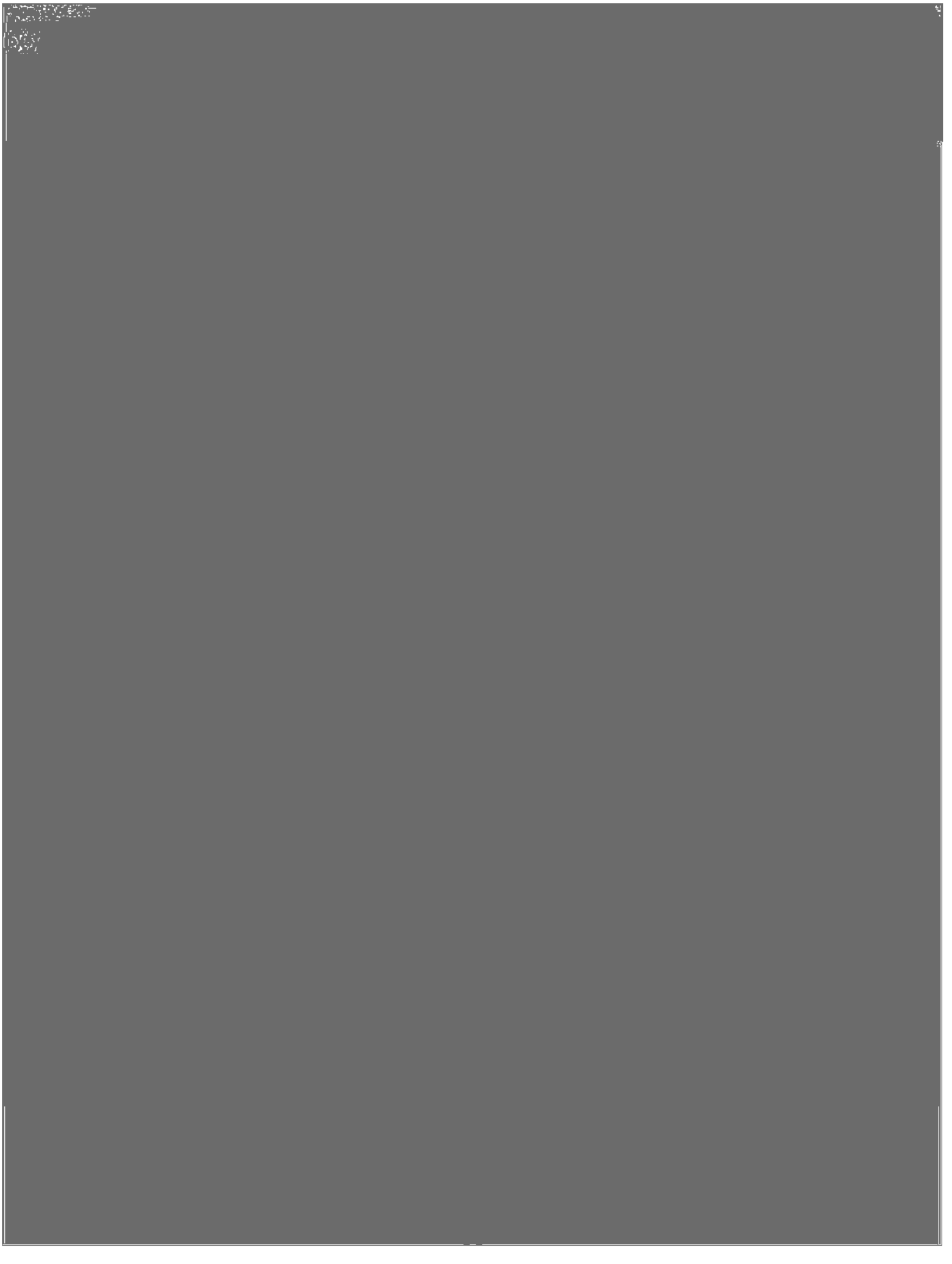


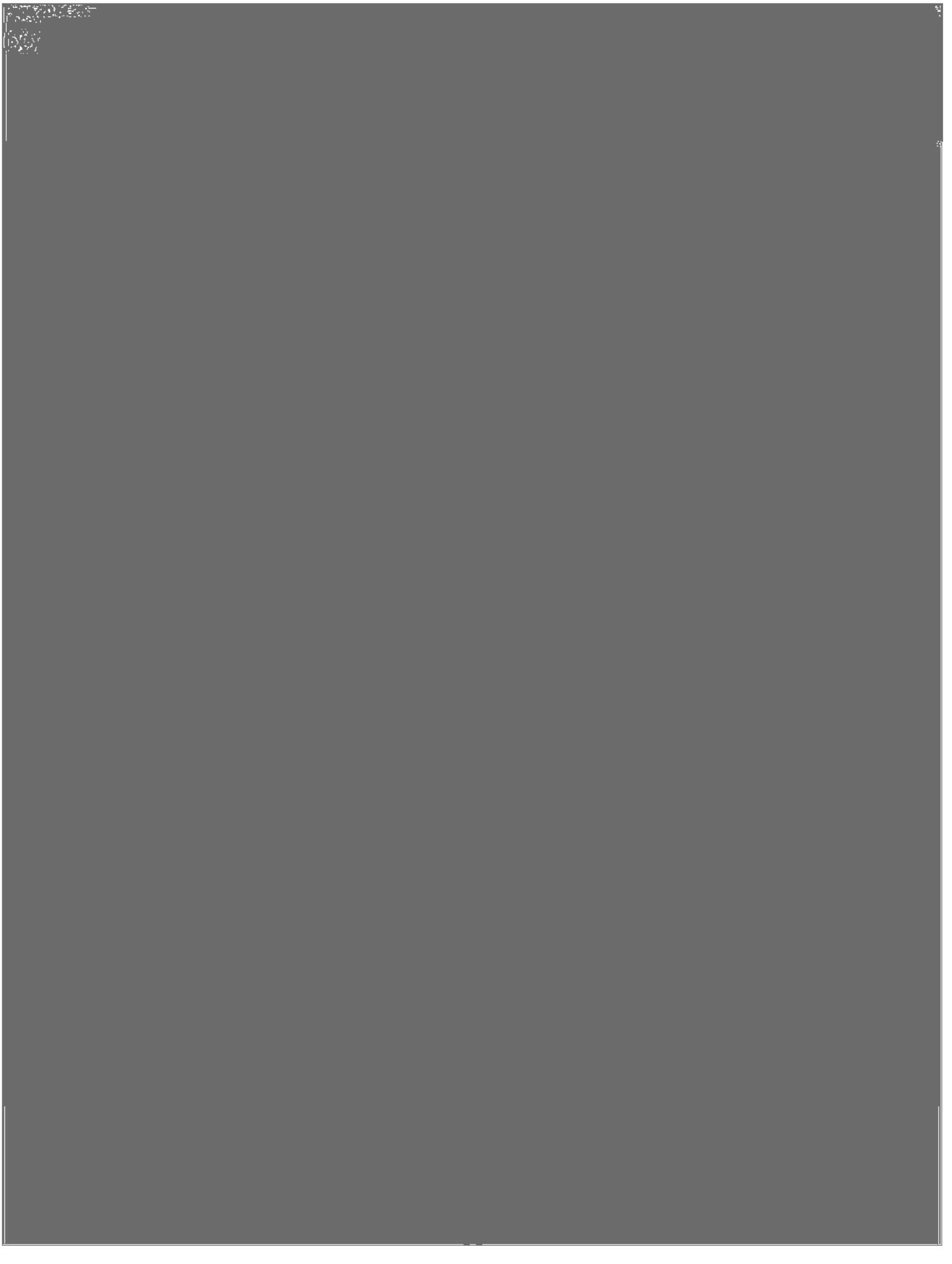


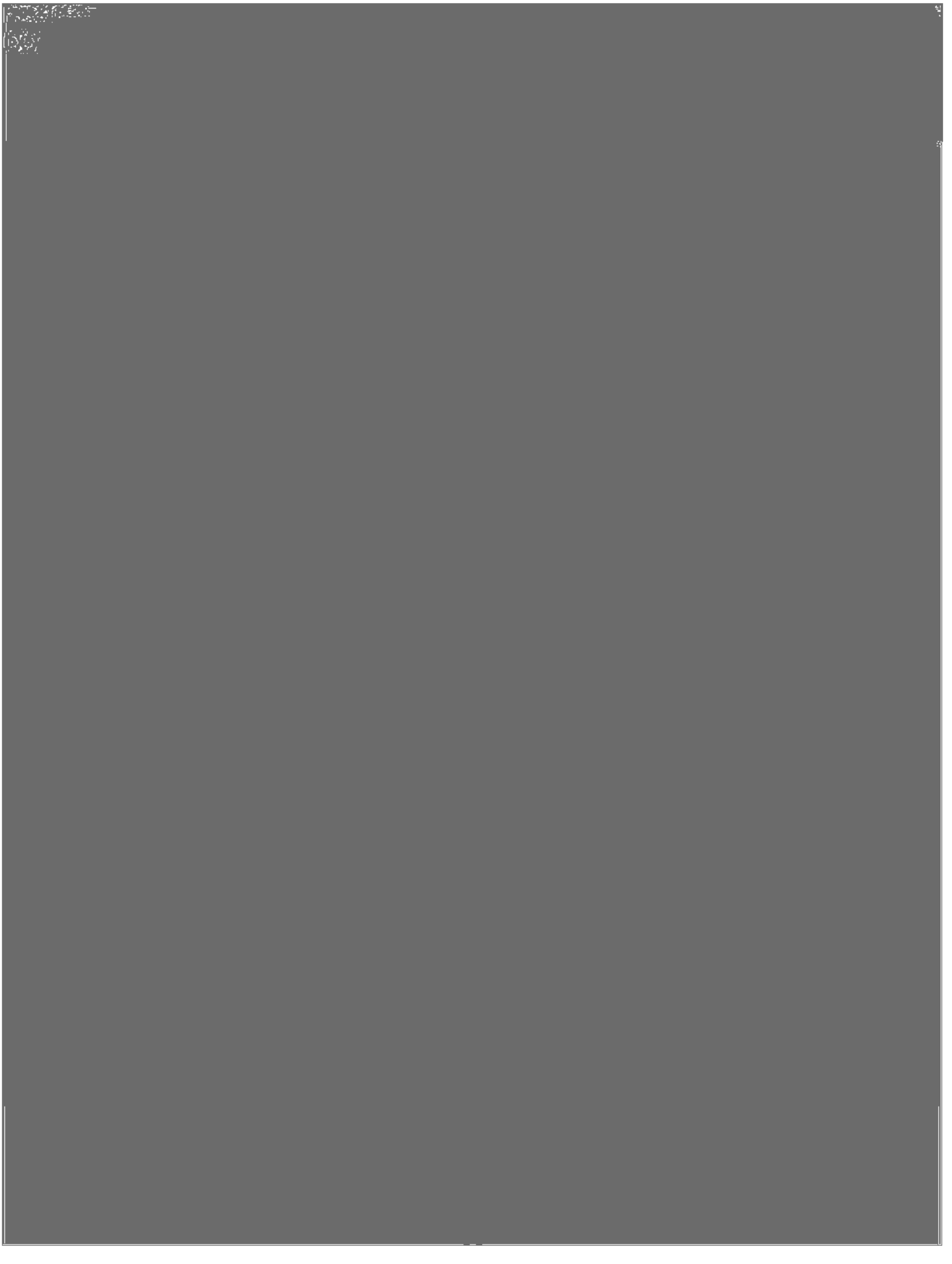


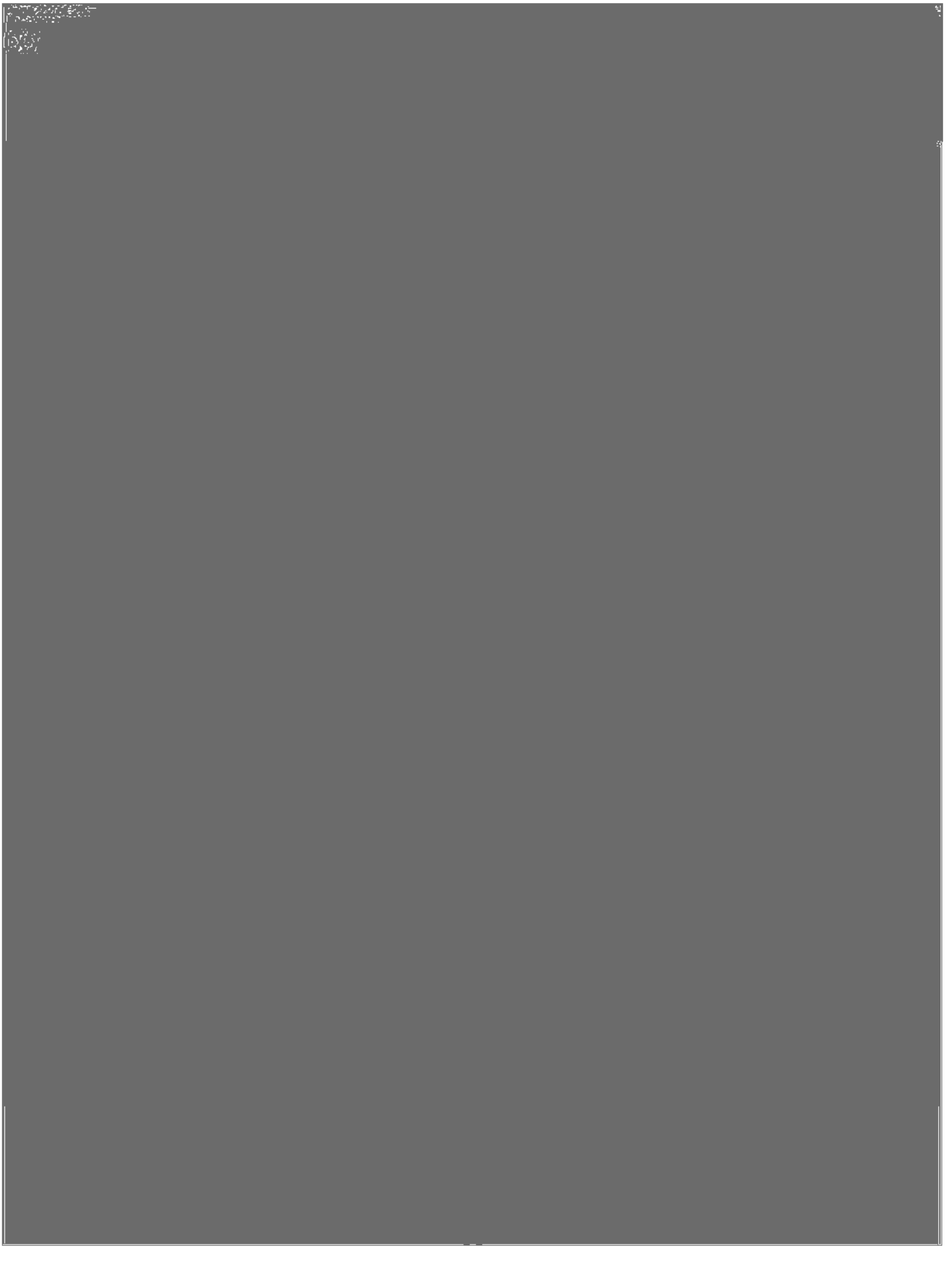
2.5 Application Migration and Sunsetting

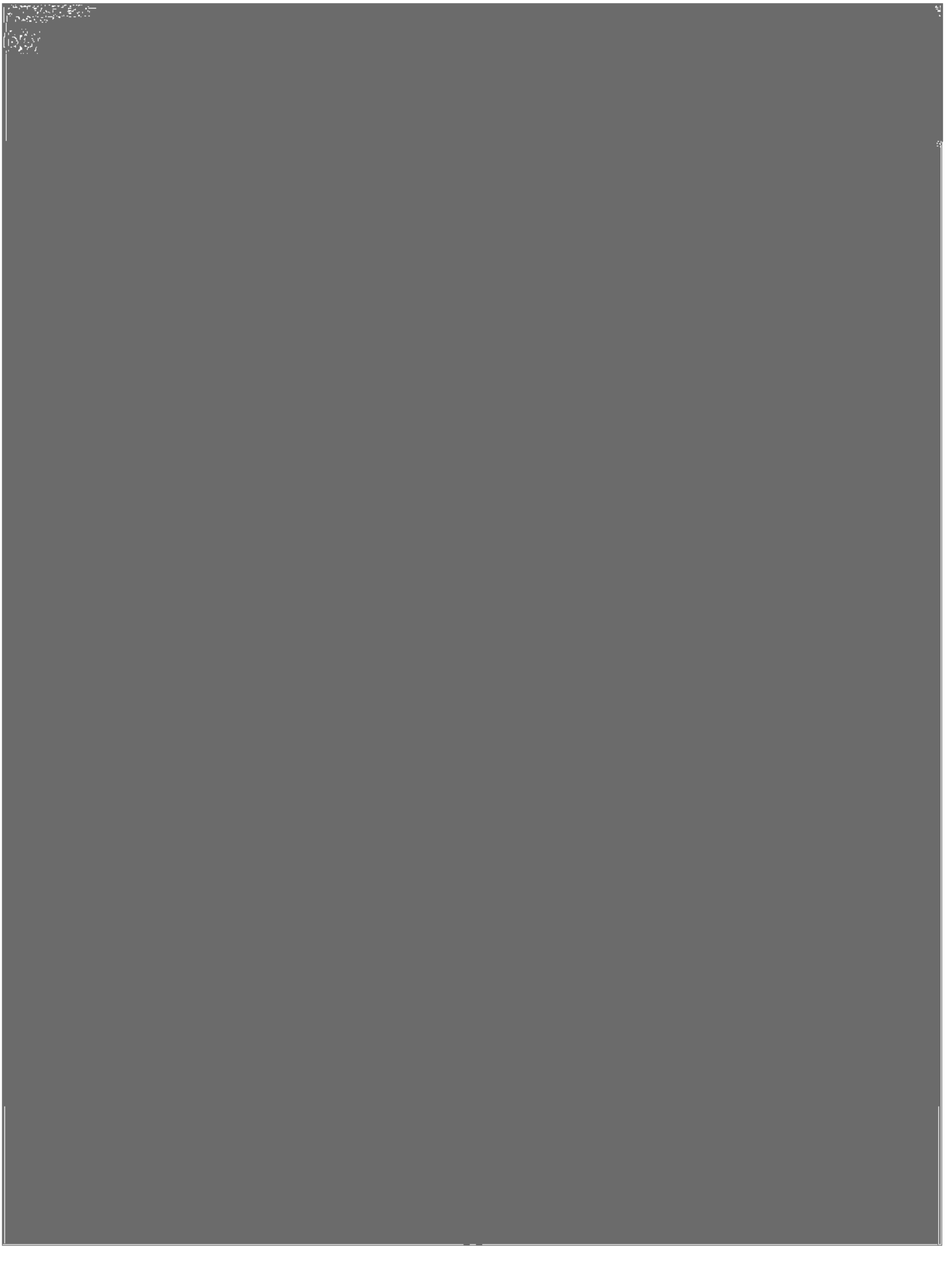
EITSD created a pilot in FY 14 to create a virtual data center using DISA milCloud service. Once the pilot is completed, EITSD will start migrate its applications to this new environment, which is anticipated to happen in FY 15. Additionally, EITSD will work with PFPA and OSD Components to develop a project with detail timeline to migrate the systems listed below to this new environment. As a result, these systems will not meet the 4th Quarter FY 18 as directed.

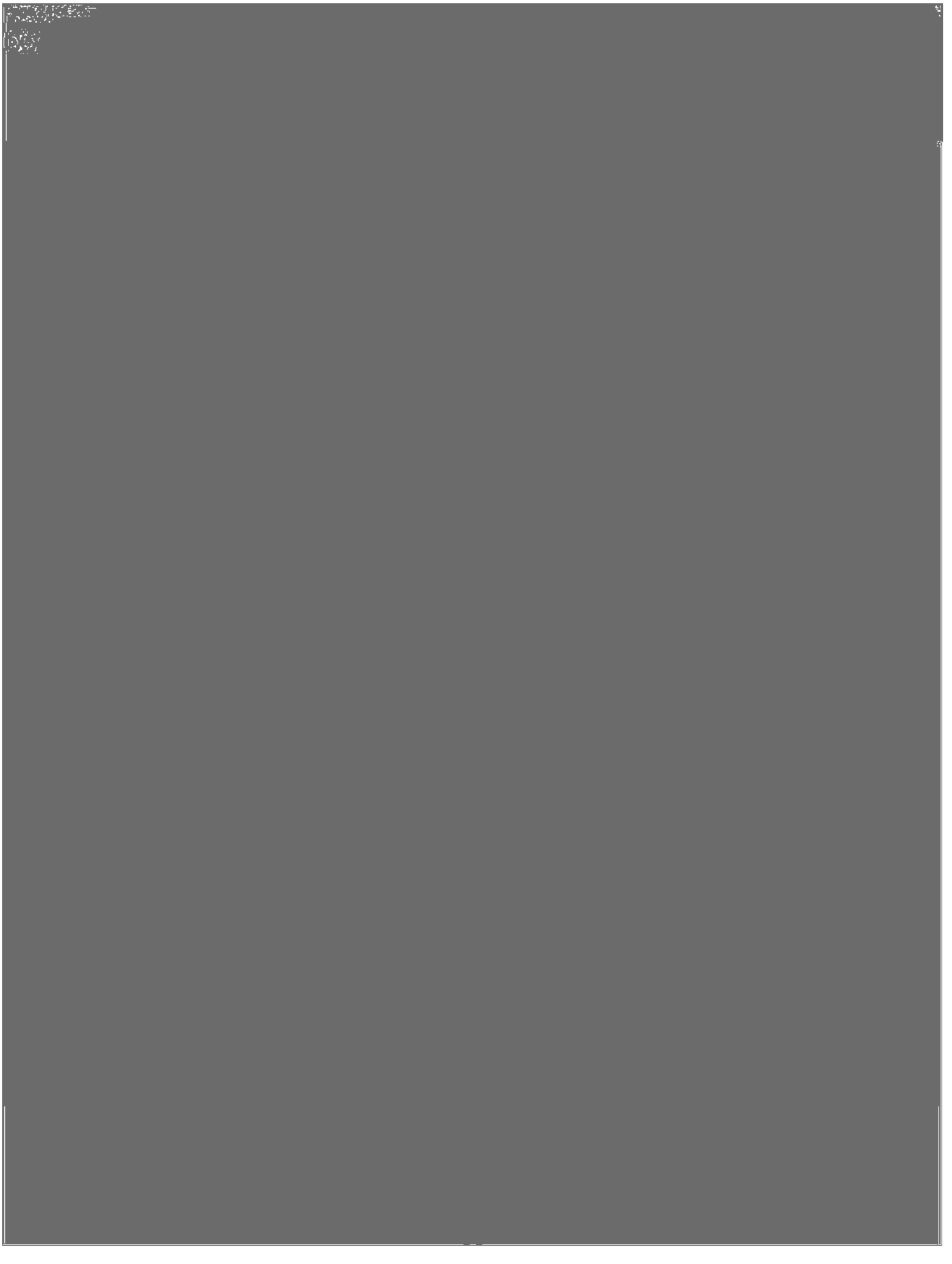












2.6 IPNs

EITSD does not manage an IPN.

2.7 ISNs

EITSD does not manage an ISN.

2.8 GSUs

EITSD does not manage a GSU.

2.9 Enterprise License Agreements

The following enterprise license agreements were used or will be established:

ELA Name	Date (QnFYyy)	Funding Source
Adobe ELA	Q4FY15	007-000003979
Direct Award to Quest ELA	N/A	007-000003979
Direct Award to VMWare ELA	N/A	007-000003979
Microsoft Joint ELA	N/A	007-000003979
Oracle ELA	Q4FY15	007-000003979