OCTOBER 18, 2017

CORPORATION FOR NATIONAL & COMMUNITY SERVICE (CNCS) MANAGED INFORMATION TECHNOLOGY SERVICES (MITS) CALL ORDER 0010 OPERATIONS AND ENGINEERING SUPPORT

The Original SOW for 0010

Contents

SECTION A– SERVICES

1 SCOPE OF WORK

The scope of this proposal includes all activities (end-to-end) necessary to provide efficient, effective and responsive IT services to support CNCS. This scope includes lifecycle activities for planning, implementing, operating, improving and sun-setting new and existing infrastructure and services within the CNCS environment.

This proposed work is within the scope of the MITS Blanket Purchase Agreement paragraph(s):

4.1. Shared Services
4.2. Facility Services
4.3 Solutions Planning Services
4.4 Infrastructure Services
4.5 IT Service Management Services
4.6 Business Services

Contractor shall provide all services necessary to satisfy CNCS requirements, in a dynamic environment for: 1) provision and operations of the MITS infrastructure and associated engineering and management professional services and 2) professional services to broker and manage a Cloud Service Providers (CSP). Contractor shall meet all the requirements contained within the CNCS BPA MITS Technical Requirements document at Attachment 1.

Shared Services

The Federal IT Shared Services Strategy defines an IT shared service as: *An information technology function that is provided for consumption by multiple organizations within or between Federal Agencies. There are three general categories of IT shared services: commodity, support, and mission; which are delivered through cloud-based or legacy infrastructures*, as is shown in **Figure 1: IT Shared Service Model** which has been adapted for CNCS[1].

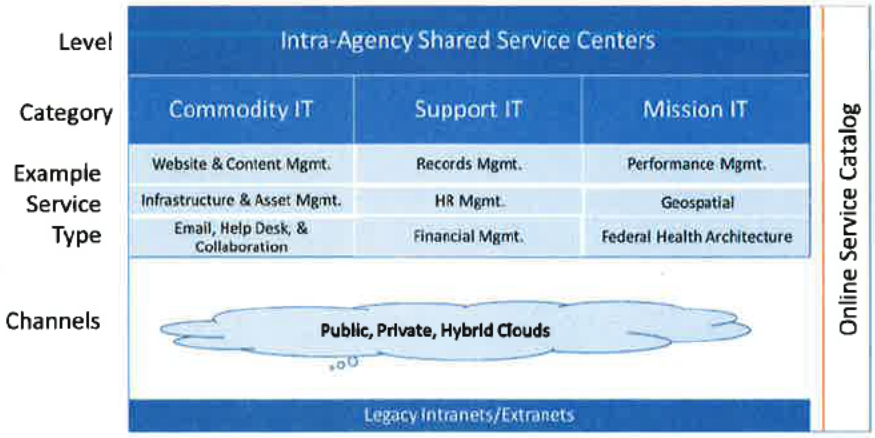


Figure 1: IT Shared Service Model

Cloud and virtualization integration engineering, optimization, and Tier 3 support will be provided by Contractor

1.1.1 CLOUD SERVICES

Contractor shall propose a solution, which can leverage any combination of service delivery options. The services will be delivered in any type of combination of cloud services to deliver and support CNCS computing requirements leveraging the essential characteristics of cloud computing should Contractorchoose to propose such a solution.

[1] Note: Not all service types will be provided under this BPA.

Contractor shall propose a combination of services that deliver the required capabilities in the most effective and efficient manner. These capabilities will promote the program objectives and outcomes to the best extent possible.

Contractor shall support production and non-production computing environments for the agency and their Contractors. Contractor shall leverage the best approach to build and support temporary or permanent non-production environments in the most cost effective and timely manner suitable to the agency and the users of these environments as the demand dictates.

1.1.2 SERVICE STRATEGY

Contractor shall assess each service and determine an appropriate cost effective, secure and optimize service delivery model while assessing and mitigating risks. The service model will use a combination of cloud services (private, hybrid, public) offerings that will provide optimal performance, agility and availability for each service.

Contractor shall expand on how additional existing or new services can be quickly and cost effectively provisioned to meet stakeholders requirements in a timely manner.

The service strategy will outline how Contractor shall design, build and integrate a computing environment capable of sustaining all services delivered to CNCS including the delivery and support from third party service providers in a timely manner. The strategy will define how Contractor shall meet the performance and availability specifications for service delivery.

1.1.3 SECURITY OPERATIONS CENTER

Contractor shall follow and remain compliant at all times with Federal IT Security standards, policies, and reporting requirements, as well as all CNCS IT Security Policies and all National Institute of Standards and Technology (NIST) and Federal Information Security Management Act (FISMA) standards and guidelines, and other Government-wide laws and regulations for the protection and security of Government Information.

Contractor shall support traditional SOC activities to protect, detect, respond to, and recover from Information Security (IS) threats to CNCS systems. SOC tasks include advising CNCS of proper security measures, encouraging industry best security practices, managing telephone trouble calls, issuance of Information System Security (ISS) Alerts, Advisories, Bulletins and ISS related information messages, incident handling and response, intrusion detection and analysis support, forensics, and metrics reporting. Contractor shall provide authorized government personnel with access to the security tools, dashboards and reports.

Contractor shall provide personnel and management in support of all CNCS security requirements to improve the overall security posture. No tools or management systems will be used in support of this effort without COR's approval. The Government requires SMEs in support of specific security initiatives. Currently these include wireless, mobility, and security system integration. There will be future systems that are not currently defined; the SMEs will be integrated into the Infrastructure and Security Engineering teams as a vital part of the system project.

1.1.3.1 SECURITY SUPPORT

Contractor shall perform the following services:

1. **Security Support**
    a. Support Tier 3 incidence response.
    b. Operate and maintain security tools to ensure an acceptable level of security. CNCS has the final authority to determine if the tools, the operation, and reporting generated by the tools are sufficient to meet CNCS security needs.
    c. Operate and maintain the Host Intrusion Detection implementation at CNCS. Contractor shall be responsible for responding to alerts generated by the host intrusion detection system (HIDS). Events, incidents, and Contractor's response to the same are all reportable events.

   d. Support the daily operations and engineering tasks; reviewing and providing recommendations in regards to all changes proposed and approved for the network such as Security Impact Assessment reports.

2. **Vulnerability Scanning** - Contractor shall perform weekly, monthly and ad-hoc security scans of systems in support events including deployments, projects, and incident response in accordance with recommended CNCS procedures, ANSI, NITS, FIPS and FISMA recommendations and guidance.

3. **Wireless Intrusion Detection** -Operate and support the centralized wireless intrusion detection implementation at CNCS. Events, incidents, and the Contractor's response to the same are all reportable events.

4. **Network Intrusion Detection**
   a. Support the operation and maintenance of the Network Intrusion Detection infrastructure. Events, incidents, and Contractor's response to the same, are all reportable events.
   b. Operate and maintain the enterprise antivirus implementation for the CNCS infrastructure.

5. **End Point Protection** - Operate and maintain the end point protection system of defense in depth to ensure the security of CNCS assets. Contractor shall take a proactive position with regard to End Point Protection controls and respond appropriately to alerts generated. All machines having generated alerts are subject to be taken offline and rebuilt / replaced at the discretion of CNCS.

6. **Enterprise Host Intrusion Prevention / Firewall** - Contractor shall be responsible for the operation and maintenance of the enterprise host intrusion prevention and firewall implementation for the CNCS infrastructure and align this with CNCS's Trusted Internet Connection (TIC) effort.

7. **Enterprise Anti-Spyware** - Contractor shall be responsible for operating and maintaining the enterprise host anti-spyware implementation for the CNCS infrastructure.

8. **Baseline Compliance and Monitoring**
   a. Create, document, and maintain baseline images and configurations that are compliant with current government standards or have CNCS approved exceptions, utilize approved change management procedures, and monitor the environment for unauthorized changes utilizing an automated compliance monitoring solution. Changes, sanctioned and otherwise, as well as Contractor's response to those changes, are all reportable events.
   b. Operate and maintain security tools to ensure an acceptable level of security. CNCS has the final authority to determine if the tools, the operation, and reporting generated by the tools are sufficient to meet CNCS security needs.

b4

[redacted]

1.1.3.2 SYSTEM SECURITY MANAGEMENT SERVICES

Contractor shall operate, maintain, and update the CNCS infrastructure so that it meets and is in full compliance with FISMA along with CNCS guidance.

Contractor shall ensure IT applications operated on behalf of CNCS are fully functional and operate correctly on systems configured in accordance with CNCS security requirements. Contractor shall use *Security Content Automation Protocol (SCAP)*-validated tools to ensure its products operate correctly with baseline configurations and do not alter applied settings (see http://nvd.nist.gov/validation.cfm). Contractor shall test applicable product versions with all relevant and current updates and patches installed. Contractor shall ensure currently supported versions of IT products meet the latest baseline major version.

Contractor shall operate, maintain, and update the CNCS infrastructure so that it meets and is in full compliance with Federal and CNCS security rules and regulations. This includes ensuring systems security for network environments, applications, databases, internet, portal and intranet that allows access only by authorized users, prevention of unauthorized release of information, prevention of degradation due to circumstances such as unauthorized internal use and external intrusion, maintenance of data integrity, and authorized utilization by the user community.

1.1.3.2.1 COMMON SECURITY CONFIGURATIONS

Contractor shall apply approved security configurations to the enterprise that are used to process information on behalf of CNCS.

Contractor shall ensure:

1. IT applications designed for end users run in the standard user context without requiring elevated administrative privileges.
2. Hardware and software installation, operation, maintenance, update, and patching will not alter the configuration settings or requirements.
3. Servers, desktops, and laptops operated on behalf of CNCS include *Federal Information Processing Standard (FIPS) 201*-compliant (see http://csrc.nist.gov/publications/PubsFIPS.html), and comply with FAR Subpart 4.13, Personal Identity Verification (PIV).
    a. Future T&M purchases of desktops and laptops will include Homeland Security Presidential Directive 12 (HSPD-12) card readers
4. Microsoft Windows-based software should use the *Windows Installer Service* for installation to the default appropriate OS Program Files directory, and should be able to silently install and uninstall, under central administrator control.

1.1.3.2.2 TRACKING AND CORRECTING SECURITY DEFICIENCIES

Contractor shall track and correct any applicable information security deficiencies, conditions, weaknesses, findings, and gaps identified by audits, reviews, security control assessments, and tests, including those identified in FISMA audits, Statement on Standards for Attestation Engagements (SSAE) No. 16 , Inspector General (IG) audits and reviews, other applicable reviews and audits, and the CNCS ITCC continuous monitoring activities such as, but not limited to, vulnerability and compliance scanning of all the CNCS information systems.

1.1.4 SECURITY DELIVERABLES

Contractor shall provide the following security deliverables:

1. Ad-hoc Security Audit Resolution report - Contractor shall conduct monthly audits on the configuration of security event monitoring devices. Monthly audits must include, but are not limited to security policy changes, account

changes (account creation, deletion, and privilege assignments), and admin changes. Contractor shall detail progress towards remediation from the results of audit findings.

2. Vulnerability Assessment Reports - Vulnerability Scanning, Tracking and Results Reporting – Bi-weekly scan for vulnerabilities in accordance with implemented organizational policy. Report non-compliant findings in accordance with established CNCS procedures.
3. Forensics Procedures and Reports – Incident Response procedures have been updated, and Contractor personnel will receive annual training on taking basic steps to maintain appropriate evidence chain of custody to support investigations. Computer investigation support involving complex data recovery as digital evidence will be contracted out to third party as ODC or for additional Contractor support through T&M when necessary. Contractor shall provide investigative support to CNCS designated staff for administrative, criminal, and matters of State as requested. Investigations into computer related events including intrusions, anomalies, misuse, and compliance issues will be conducted when requested by CNCS designated staff. Support for administrative investigations, when directed by the appropriate authority, will be conducted in accordance with forensically sound procedures and best practices. This does not require the legal framework involved in criminal proceedings, however, computer investigation support must be conducted in a manner which can be utilized by law enforcement in the event that criminal conduct is suspected. At the completion of each event, Contractor shall publish a standardized report to be distributed within two days of event completion, at the direction of the CISO. The report must detail all investigative activities, actions taken in response to the incident, and a detailed accounting of all equipment affected.
4. Incident Response Report - Contractor shall act as a subject matter expert in log analysis for identifying security incidents, policy violations, and malicious code. Contractor shall prioritize its resources for analysis of security logs to detect incidents on the CNCS network (except as directed by the CISO), and assist in remediation. Contractor shall follow all CERT guidelines for reporting incidences.
5. Security Summary Report - Contractor shall create the following trend reports which will be submitted to CNCS on weekly, monthly or as required basis:
   a. Security events prioritized by threat level;
   b. Open and closed incidents;
   c. Blacklist of suspicious source IP directed at CNCS targets;
   d. Forbidden or suspicious protocols and ports active on the CNCS Network;

b4 [redacted]

   i. Top 5 Continuous Improvement report for configuration and vulnerability issues;

b4 [redacted]

- Top 10 Web Blocked Sources by IP Address
- Top 10 Web Blocked Sources grouped by Network (subnet)
- Top 10 Sources IPs/Countries of Foreign Attacks
- Top 10 Destination IPs/Countries of Foreign Attacks

6. Scanning Reports - A top 5 issues report for continuous improvement utilizing the results of configuration and vulnerability scans will be provided to CNCS designated staff. This will be updated weekly.
7. The Contractor shall provide a Security Operations Procedure Plan within 60 days of award. The plan shall include:
    a. Workstation, server and network device hardening requirements (e.g., established baseline based on CNCS Cybersecurity policies and procedures)
    b. Types of events or activities which constitute a Security Incident
    c. Functions of the operating environment
    d. Incident response priorities and processes to mitigate damage
    e. Privacy breach protocol including, but not limited to breach notification process
    f. Processes to monitor for system security vulnerabilities and to apply security patches accordingly

1.1.5 SECURITY SUBJECT MATTER EXPERTS (SMEs)

Contractor shall work with other CNCS personnel and Contractors to oversee the remediation of identified security issues within the CNCS network. CNCS expects Contractor to oversee the resolution of security issues including determination of the remediation steps in accordance with applicable CNCS SOC SOPs, CNCS/HHS policies and direction from the CISO. Contractor shall provide subject matter expertise as well as assist the CISO and government staff in determining the appropriate corrective action for new and evolving scenarios and develop/document those corrective actions as part of the maintenance of the CNCS SOC SOP repository. The documentation of the corrective action recommendations will be provided within three (3) days of scenario discussion. Remediation will be captured as Plan of Action and Milestones (POA&Ms) and performed and reported in accordance with SLA's and /or Federal Security Requirements.

1.2 FACILITY SERVICES

b4

b4

[redacted]

b4 [redacted]

1.3 SOLUTIONS PLANNING SERVICES

1.3.1 ANALYSIS AND REQUIREMENTS

b4 [redacted]

b4 [redacted] As part of the Solution Planning Services Contractor shall determine the best fit most cost effective outsourcing strategy for supporting all of the services. Contractor shall manage the services or may choose to outsource all (or none) of the services and functions to subContractors, which would deliver the services and functions under the supervision and control of Contractor . Contractor shall be responsible for ensuring that all third parties are capable of supporting the services and meeting or exceeding the performance and availability SLAs for the services they deliver.

1.3.2 CAPACITY PLANNING

Contractor is responsible for production capacity allocation and will manage the allocation of capacity for the CNCS solution including:

- Managing the allocation of existing fixed capacity
- Monitoring the performance and throughput or load on all aspects of the CNCS platform
- Performing tuning of environment and activities to ensure the most efficient use of existing infrastructure

Contractor shall monitor system utilization and estimate capacity requirements for processing, licensing (hardware/software), storage and communications based on analysis of observed trends and CNCS program plans.

Contractor shall follow all CNCS and ITIL change management control processes. Contractor shall also provide a system that documents any changes made to any systems to which authorized government officials have access.

1.3.3 SUPPLY CHAIN MANAGEMENT

Contractor shall be responsible for the procurement of all resources and services required to deliver effective and efficient operations and engineering services. b4 [redacted]

b4 [redacted]

b4 [redacted]

b4 [redacted] Contractor shall be responsible for the provisioning, integrating, testing and operational support for the solution services. Contractor shall ensure that all suppliers and sub-Contractors can provide the necessary resources, and that all resources that require licensing are properly licensed and used according to the terms of the licenses. Contractor shall ensure that additional resources can be quickly provisioned to handle increased demand in services or the deployment of new services.

Contractor shall perform technology assessments of new hardware and software to ensure the most appropriate versions of hardware and software are in use. Contractor shall maintain the technical currency of all Contractor provided assets in accordance with CNCS standards, CNCS operating requirements, and then-current OEM standards. Additionally, Contractor shall provide recommendations to the Government, accompanied by the supporting business case and costs for improvements, enhancements, and upgrades to any Government-owned and/or Government-provided hardware and software. Contractor shall make recommendations to improve third party services, whether directly contracted with CNCS or provided by their own sub-Contractors which may improve the effectiveness, efficiency and costs for these services.

b4 [redacted]

1.3.4 SOLUTION DESIGN

b4 [redacted]

1.4 INFRASTRUCTURE SERVICES

Contractor shall support CNCS services in a fault tolerant, cost effective configuration. The architecture will define a comprehensive computing solution, designed, built, integrated, managed and operated by ContractorR. The architecture will, at a minimum, maintain the confidentiality, integrity and availability of the data and systems. The architecture will support all of the current CNCS services running at the existing data center. Changes to the architecture will require CNCS approval before implementation unless agreed upon and documented by the government. Contractor shall be responsible for the complete implementation of the architecture.

The architecture will leverage current and emerging technologies to provide a secure and stable computing environment. The architecture will be based on the current platforms and solutions in use at the existing MTIPS; if Contractor chooses alternative platforms and solutions, Contractor shall demonstrate that the functionality remains intact and will be delivered at the expected or improved service levels. Contractor shall suggest recommendations for changes to the current computing environment that would improve performance, availability, stability, security and reduce operational risks, complexities, resources and costs.

The service architecture will leverage tools and performance metrics to illustrate improvements in performance and quality of services. The services will be continuously monitored for service failure, degradation, and instability and provide real time (or near real time, although real time is preferred) status indications through a web based dashboard view which can be viewed by authorized CNCS and managed by Contractor's Service Operations Center(s).

Contractor shall procure and manage all hardware, software and service resources required to meet or exceed the Service Level Agreement parameters for MITS as agreed by CNCS and Contractor. Provisioning of the resources will be the responsibility of Contractor.

Contractor shall maintain the proper level of staff resources knowledgeable in the technologies in use. The Contractor staff resources will have domain knowledge of the CNCS computing environment. All changes to the architecture will be updated to reflect the current environments.

The architecture for the computing environments will be tailored to meet the performance and availability demands for each service. The production environment will support high availability of services to meet the minimum uptime requirements as those of a Tier 3 data center. Uptime includes a performance degradation of no more than 10% of expected service levels.

Contractor shall provide services to manage all CNCS infrastructure operations and maintenance. The operations support staff will be a blend of remote and onsite personnel.

Contractor shall perform all regular maintenance on CNCS Infrastructure to include patches, hardware, and system upgrades. The monthly hardware maintenance includes the installation, testing and implementation of OS and security patches, OS release upgrades, firmware upgrades, application installation and upgrades, and other infrastructure software patching for all systems. Other scheduled maintenance and support services that may affect customer access to servers that cannot wait until the next maintenance period will be performed outside of the normal operating hours as directed by CNCS. Contractor shall provide SMEs for the integration engineering, optimization and Tier 3 support of Infrastructure O&M.

1.4.1 SERVICE HOSTING

Contractor shall:

1. Provide network management services at CNCS headquarters, Wide Area Network (WAN), Metropolitan Area Network (MAN), and Local Area Network (LAN) services in local and field offices. A comprehensive, proactive program of services is required to manage and ensure industry best practices, and cost effective operation of the network infrastructure. Services are required to configure, install, control, monitor, troubleshoot, remediate, upgrade and report on the status of all LAN, MAN and WAN components. These components include: the CNCS core backbone, fiber and copper cable routers, switches, distribution and access layer devices, load-balance switches, WLAN wireless access points and WIDS/WIPS sensors, mail routing appliances and other inter-network connection devices that provide Wireless Network Access, network De-Militarization Zones (DMZ), WAN optimization/acceleration, and secure VPN gateways. Contractor shall provide support for equipment that resides on both the Intranet and Extranet. In addition, Contractor shall provide integration engineering, optimization, and Tier 3 support for all communications requirements.
2. Install, deploy, troubleshoot, operate, maintain, and configure all network infrastructure systems to include fiber optics, switches, routers, and other equipment required to provide data connectivity to and from all activities and locations operated or supported by CNCS, with minimal interruption of services.
3. Provide support services for all data, Internet Protocol (IP) telephony and video transmissions up to the Internet Service Provider (ISP) carrier demarcation handoff, with management of carrier services limited to status monitoring, reporting and coordination during troubleshooting and repair activities.
4. Collaborate and coordinate with ISP carriers as required for any service degradation incidents to monitor, report status and assist with remediation activities. Network infrastructure incidents are defined as service availability problems that could range in severity from service degradation through lost redundancy without a complete loss of service, throughput degradation from network latency, intermittent service interruption, or complete outages.

5. Complete network terminations and station cable pulls for copper and fiber connections across the network. This includes providing network connectivity in moves, adds, and changes in end-user office spaces. Connections will be maintained for telecommunication closets, offices, network devices and miscellaneous drops in compliance with telecommunication closet standards and industry standards such as IEEE, and EIA/TIA. Network connectivity may include physical security equipment if requested.
6. Administer and optimize use of network management techniques and tools to deploy new operating systems, code, push configuration changes, capture essential information and manage device configuration files.
7. Track service and report requests that meet milestones based on operational feasibility and the urgency of requirements.
8. Manage, track and report on all IP address assignments in accordance with established CNCS guidelines and approved Information Technology Infrastructure Library (ITIL) processes. This includes the Internet Protocol (IP) Address Schema and Virtual Local Area Network (VLAN) assignments for the CNCS network. Allocation of addresses will be maintained in a repository that facilitates ease of use, administration and reporting. Repository information will at a minimum include address space, purpose, associated system, requestor, date of request and location.
9. Maintain control of the network devices with security access and authentication measures established to meet Federal best Practices. Password change management, Network Access Control/802.1x port authentication, TACACS + and other security controls will be used to ensure that only authorized users can access the CNCS network routers, switches and appliances.
10. Provide personnel experienced in advanced networking and security disciplines to keep up with next generation technologies. Examples of these technologies are network virtualization, utilizing a common switching infrastructure and next generation firewalls.
11. Network Hands-on Support - Perform any physical, "hands-on" work needed on network equipment within CNCS locations in the DC Metro area wire/LAN closets. Outside the DC Metro area "hands-on" wire/LAN closet work will be performed by CNCS field IT staff or other Contractors.
12. Perform periodic inspection and housekeeping of DC Metro area wire/LAN closets to ensure they are maintained to Industry and CNCS's standards.
13. Wide Area Network (WAN) - Provide engineering support for a fault tolerant WAN with redundant paths and POP diversity as required.
14. Operate and manage the entire CNCS core backbone, distribution, and access layer devices; load-balance switches, mail routing appliances and other inter-network connection devices; WAN optimization/acceleration appliances; WLAN wireless access points and WIDS/WIPS sensors; and secure appliances for VPN gateways. Track completed management activities and provide reporting that assists with status monitoring, troubleshooting and process improvement efforts.
15. Local Area Network (LAN) - Provide support in resolving third tier network problems; upgrade, replace, or augment network hardware and software; leverage internet technologies to support the CNCS business needs; and establish remote access capabilities.
16. Maintain all documentation and tracking systems required to manage and maintain the integrity of the network. Contractor shall provide authorized government personnel with access to this system. This includes traffic flow diagrams, design diagrams, closet layout diagrams and spare part inventories. Ensure the ongoing availability and accessibility of network topology diagrams that depict layer 2 and layer 3 switching. Layer 3 diagrams will illustrate routing protocols, Open Shortest Path First (OSPF) area boundary, Border Gateway Protocol (BGP) autonomous systems, Virtual Route Forward (VRF) and other layer 3 routing configurations. Layer 2 diagrams

will illustrate Local Area Network (LAN) and Virtual Local Area Network (VLAN) trunks, Spanning Tree, Root Bridge Assignment, Hot Stand-by Routing Protocol (HSRP) Primary/Secondary Configurations and any other layer 2 link state configurations.

1.4.2 WIRELESS COMMUNICATIONS SYSTEMS

Contractor shall

1. Manage the existing Cisco b4 [redacted] Cisco Wireless LAN Controllers and Cisco Light Weight Access Points. These tools allow for secure monitoring and configuring the wireless components of the CNCS network.
2. Support WLAN as a productivity enhancer for CNCS staff, guests, and Contractors.
3. Provide appropriate Federal Information Processing Standard for client\server software solution for all wireless network communication within CNCS.

1.4.3 TELECOMMUNICATION SERVICES

Contractor shall support the network infrastructure used to transmit data, voice, and video traffic, delivering the business benefits of converged network increased productivity, greater business flexibility, and reduced operational costs to CNCS. The standard IP telephony services typically includes the following capabilities: national dial-plan management, local and long distance call forwarding, call answering, conference call, voice messaging, international calling and speed dialing.

1. VoIP/Video - Perform the following management services:
    a. Proactive fault management
    b. Configuration Management (Move, Addition, Change, Deletion (MACD))
    c. Design, site installation, test/turn-up, and life cycle management
    d. Accounting management
    e. Performance management
    f. Performance and Service Level Agreement (SLA) reporting
2. VoIP Phone System
    a. Perform adds, moves, and deletes and maintain the VoIP user database.
    b. Log and troubleshoot all VOIP hardware and software related issues from the infrastructure to the servers to the desktop units.
    c. Second response (Tier 2 and 3) for the VoIP end user community.
    d. Installation, b4 [redacted] and testing of phones, b4 [redacted] and cabling b4 [redacted] b4 [redacted]
3. Provide support for voice trunks and other trunking solution used within CNCS for VoIP services.
4. Telephony Services - Manage, maintain, and operate existing IP telephony servers, switches, routers and other equipment supporting VoIP networks including configuration of auxiliary voice VLANS.
    a. Maintain configuration, management and operations of network devices, PSTN interface and fax modules supporting the telephony system.
    b. Support of telephony moves, adds, and changes (MACs) and complete other associated tiered Service Desk network requests.
    c. Manage and operate IP telephony services to include unlimited local connection for basic telephone functionality within CNCS, including provision of access to toll-free numbers
    d. Provide system hardware and software support to include de-installation, re-installation, and change.

e. Support telephony services with capability to support Extension Mobility, Unified Messaging, and Emergency Responder.
f. Provide end user training and education on the various telephony devices provided by the CNCS for voice services on the network, including computer‖based training, web based training, and instructor led training as required.

5. Rich Media Support/Video Teleconference
   a. Engineer, configure, certify and accredit, install, test, maintain, refresh, and coordinate all secure and non-secure VTC and Audio Visual (AV) systems and collaboration tool technology activities.
   b. Evaluate and diagnose audiovisual equipment requiring service, and identify and troubleshoot problems in such equipment.
   c. Maintain associated VTC backend equipment, including, but not limited to, multipoint control unit (MCU) and networks.
   d. Conduct initial hands-on training sessions for each new installed VTC system and for each new AV system with the principle system owner/user of each new VTC/AV system.
   e. Support and manage all Voice and Video conferencing equipment and software.
   f. Administer Voice and Video conferencing systems for campus use and potentially CNCS-wide use.
   g. Train administrators in the use and management of Voice and Video conferencing scheduling, operation, video recording, and collaboration.
   h. Troubleshoot and correct all user issues in CNCS trouble ticket system.
   i. Perform routine tests on the Voice and Video conferencing systems and end points.
   j. Coordinate all non-CNCS requests for Collaboration efforts via the Web
   k. Provide VTC training

b4 [redacted]

1.4.4 SERVERS AND STORAGE

Contractor shall provide support service for all server and storage technologies and associated infrastructure at CNCS locations. The CNCS servers support infrastructure services, applications services, and operational support (hosting services) to customers. The support level provided is detailed through SLAs. The current supported environment typically includes: Windows servers, Linux appliances, tape libraries, SANs and any hardware. In addition, hardware and software integration engineering, optimization, and Tier 3 support will be provided by Contractor. Contractor shall:

1. Support application servers, file and print servers, domain controllers, web servers, and database servers.
2. Support any future changes to the existing CNCS architecture.
3. Integrate, sustain, and provide reliable access to all servers and tools on servers, and support the uptime goals defined to achieve the business needs of the organization.

4. Support users in meeting mission requirements by managing and updating user access rights and data schemas.
5. Address issues with and configuration changes, software, and licensing.
    a. Ensure licenses are maintained
    b. Advise on industry best practices and impact of potential license upgrades
6. Coordinate testing with system owners when integrating new production releases in support of changes, enhancements, and the integration of new systems.
7. Monitor storage capacity and growth, track associated risks, and make recommendations to the COR based on risk assessments.
8. Storage Management - Provide technical support to monitor, provision, operate, expand, consolidate, and optimize the IT Storage infrastructure. CNCS requires expertise to assure the efficient transition to a consolidated enterprise environment that effectively addresses CNCS's current requirements and is scalable to accommodate future needs.

1.4.5 WORKSTATION SERVICES

Contractor shall provide a comprehensive solution for managing Agency end user computing resources (including computers, tablets, smartphones and printers). Contractor is responsible for moves, adds and changes and inventory control including shipping and receiving. Contractor shall perform installations and configuration of hardware and software, including peripherals, and coordinate repair and maintenance services.

1.4.6 MOBILE DEVICES SERVICES

Contractor shall provide a comprehensive solution for managing the Agency's mobile devices. Services include all aspects of device provisioning and management. Contractor serves as the Agency's liaison to carriers for device activation and deactivation. Telephony Support will include a national dial plan(s), moves/adds/changes, integrated voicemail and messaging and management of all licensing on behalf of the Agency. Contractor shall review monthly billing to ensure accuracy and optimum service categories. Contractor shall report usage statistics, number of users, adds, changes, deletions on a monthly basis. Contractor shall assess performance and make necessary adjustments to optimize performance.

Contractor shall be responsible for adding or updating mobile service applications and mobile OS updates. Contractor shall be responsible for provisioning new mobiles devices and disposing of obsolete and non-reparable mobile devices. Contractor shall be responsible for repairing all "reparable" mobile devices. Contractor shall be responsible for managing all devices which support mobile tethering capabilities. Contractor shall manage mobile assets, shipping, receiving, tracking and reporting the statistics such as (but not limited to) device type, count, location, service plan.

Contractor shall provide comprehensive support for all Agency furnished mobile devices, including cell phones, smart phones, tablets or any other type of portable device. Contractor shall support OS upgrades, application management, patch management, deployments and configurations. Contractor shall coordinate mobile broadband activation and include mobile devices, phone numbers, electronic serial numbers and other radio identifiers in the system inventory. Contractor shall review utilization statistics and optimize plans to derive cost efficiencies.

1.4.7 MANAGED PRINT SERVICE

Contractor shall provide support for Agency desktop and network printers, scanners and multi-function devices. Contractor shall support CNCS Facilities Services and coordinate with 3rd party vendors to support non-OIT managed copiers. Contractor is responsible for adds, moves, changes and inventory control including shipping and receiving. Contractor shall act on the Agency's behalf to schedule and coordinate installations, repairs or maintenance services. These maintenance services will include the design, development and deployment of technologies to facilitate support to the Paperwork Reduction Act. This has been accomplished by implementing Follow-Me-Printing and Personal Identity Verification (PIV) Card enabled printing technologies.

1.4.8 HARDWARE ASSET MANAGEMENT SERVICE

Contractor shall provide a complete hardware lifecycle management solution for Agency hardware assets. Managed hardware assets include, but are not limited to:

- PC desktops, Laptops, Monitors, mobile devices, Docking stations, Desktop printers, scanners, multifunction devices, Routers, Switches, Uninterruptable Power Supplies, Headquarters equipment, Network printers, scanners, multifunction devices, Mice, keyboards, trackballs, cameras, and other peripherals, Telephone stations, Conference stations, VTC equipment
- Assorted supplies such as toner, batteries, cables, power strips

Hardware management will include property receipt, inventory control, equipment staging and distribution, coordinating warranty repairs, and final erasure and transfer or destruction. Contractor shall maintain a complete inventory database including, make, model, serial number, user assignment, locations, warranty and purchase records. Contractor shall deliver quarterly reports of all hardware assets as well as any disposal of assets.

Contractor shall provide packing, labeling, and transport for hardware assets to/from loading docks, supply rooms, and mail rooms within the headquarters facility. Contractor shall report and manage equipment damage claims with transport carriers on behalf of CNCS. Contractor shall provide shipping cartons and labels as required for remote office support using CNCS provided supplies.

Contractor shall maintain physical security and asset lock-down kits. This includes, but is not limited to keyed cable locks, combination locks, device anchors and secure key and combination assignment and management. Contractor shall ensure unique combinations are used with combination locks and provide forgotten combination assistance for authorized users.

Additionally, Contractor shall use the Agency's LAN Desk management suite, or equivalent, to discover and gather automated inventory data. Contractor shall perform routine discovery and maintain equipment assignment information.

Contractor shall provide:

1. Annual physical inventory
2. Detailed hardware and software reports upon request

1.4.9 HELP DESK SERVICES

Contractor shall provide help desk services to CNCS staff during core business hours (8:00am – 8:00pm EST) Monday-Friday. Support from 6:00 PM to 8:00 PM will be in the form of phone support. During the six weeks prior to the end of the Government Fiscal Year the help desk service hours will be from 8:00 am to 12 midnight on week days and from 10:00 am to 5:00 pm on weekends. Service Desk staff will escalate unresolved issues to on-site desk-side support staff located at CNCS headquarters in Washington, DC. Contractor shall respond to help desk inquiries from CNCS computer users by providing technical assistance, support, and advice. Contractor shall interpret problems and provide technical support for hardware, software, communications, and systems. Contractor shall install, modify, clean, and support computer hardware operationally and software. Contractor shall provide help to CNCS staff on topics including but not limited to:

- Account creation/maintenance
- Login/logout
- Data storage/transfer
- E-mail
- Microsoft Office 365
- Network printing
- Communications (Internet/Intranet/network/faxing/telecommuting)

- Account lock-out assistance
- Virtual Private Networking and Remote Access
- Voice Over Internet Protocol (VOIP) use questions
- Equipment setup/configuration/distribution/installation
- Equipment inventory (hardware/software)
- Local security (virus protection/spyware/authentication)
- Training support (write training manuals and train computer users in how to use new computer hardware and software as requested)
- Premise Wiring from patch panel to wall jack to telephones, computers and docking station

Tier III level service under this requirement is for client based support only.

Contractor shall:

- Implement ITIL v3-compliant processes and tools
- Perform request management, including:
  - Answer calls within performance standards specified in Service Level Agreements (SLAs)
  - Create tickets and gather information including verification of end users computer serial number and/or asset tag to ensure inventory for the caller is accurately reflected in the asset management database
  - Determine the impact or urgency of the request
  - Assign appropriate priority using approved classification standards
- Resolve request based on SLA performance metrics
- If needed, forward the request for resolution to Tier II or Tier III personnel as appropriate
- Inform user of action to resolve request or provide an estimate of resolution time period (if request not resolved during call)
- Resolve service requests, including:
  - Assign and resolve pre-approved change requests within SLA performance standards
  - Perform desk side and account services
  - Install, upgrade, or modify hardware or software as required
  - Record actions in trouble ticket system
  - Resolve informational requests or questions based on agreed scripts (e.g., for Frequently Asked Questions [FAQs]) or other sources
  - Record special requests, request approval to comply with requests, assign and resolve approved requests, and report results
- Resolve incident reports, including:
  - If possible, resolve the incident at first contact (Tier I)
  - As appropriate, record the incident in the Known Error Database
  - If required, transfer responsibility for resolving the incident report to Tier II staff to: investigate the problem; as needed, provide desk side support to the user; and update the Known Error Database
  - If required, transfer responsibility for resolving the incident report to Tier III staff to: investigate the problem; develop and implement a solution or workaround, fix the incident in place; as needed, route the incident to problem resolution; and update the knowledge base once fully implemented
- Resolve problems that cannot be adequately corrected through on-site repairs or workarounds, including:
  - Investigate the problem and perform root cause analysis on Severity 1 problems

  - Develop a permanent solution to the problem
  - Submit a Change Request to implement the solution if applicable
  - If approved, perform the implementation of the solution
  - As possible, resolve the incident at first contact (Tier I)
  - As appropriate, record the incident in the Known Error Database
- Perform closeout activities, including:
  - Update and close the trouble ticket
  - Report actions to the user
  - Generate reports of request and resolution
  - Request user complete brief customer satisfaction survey

Contractor shall:

- Monitor resolution of Help Desk [redacted]
- Perform trend analysis of Help Desk incidents
- Perform root cause analysis of incidents
- Perform analysis of the effectiveness of corrective actions in preventing similar problems
- Maintain a complete, accurate, and up-to-date database of requests, actions, and results
- Report Help Desk performance data as part of periodic performance reports
- When appropriate, notify CNCS officials of service requests or incidents based on agreed request priority and problem resolution procedures

Contractor shall identify areas for improvement in Help Desk services, including total cost of ownership (TCO), response and resolution times, and customer satisfaction

1.4.10 DAILY INCIDENT/SERVICES DEGRADATION/OUTAGE REPORTS

The Contractor shall present a daily Incident/Services Degradation/Outage report, which will be subsequently rolled up into a weekly, monthly, quarterly and yearly incident report/summary.

The daily incident report will include items such as, but not limited to, number of incidents reported, number of incidents resolved, number of incidents still open {and their status towards resolution which should also include information about systems and stakeholders currently affected by the unresolved incident) and the severity level of the incidents.

The Incident/Services Degradation/Outage Reports at a minimum should contain:

- Root cause analysis {RCA)
- Service{s) Impacted
- Application/System/Server{s) Impacted
- Start time
- Service restored timestamp
- Duration (minutes)
- Method of detection
- For sevlce incidents a RCA must be completed within 72 hours of resolution

A more detailed incident report for each incident, based upon the incident ticket, shall be made available to CNCS by the Contractor upon request. In addition to the daily incident report, the Contractor shall immediately notify the CNCS upon learning of any significant issue with the performance of any component of the enterprise: applications, systems, the network, etc. The Contractor shall work with the COR to determine communication protocol during significant incidents. The weekly incident report shall be a roll-up summary of the previous daily reports (and would be presented weekly or bi-weekly, at CNCS discretion), while the monthly incident report would include further analysis such as average number of incidents per day, mean time to close, percentage of first contact resolution, etc. The quarterly and yearly incident reports shall be rolled-up summaries of the monthly incident reports, with some added "year-over-year" and "comparable time period" (i.e. Second Quarter (Q2) last year vs. Q2 this year) analysis.

The information presented in the various incident reports shall also be available via a browser-based dashboard accessible by authorized CNCS authorized government personnel.

1.4.11 SYSTEMS AVAILABILITY REPORTS

The Contractor shall present a browser-based dashboard in real-time or as near real-time as possible reporting on the availability of major systems as defined by the CNCS. This dashboard will indicate the up/down status of major systems, and also the running uptime average, i.e. for the past month or quarter, of the major systems. This real-time report should be generated automatically from monitoring and managing systems data.

This dashboard will be drillable down for more detail and will be made available to authorized CNCS government personnel.

1.4.12 PERFORMANCE REPORTS

The Contractor shall provide the COR with performance reports on an ad-hoc and scheduled basis (monthly, quarterly, semi-annually, and annually). All reports should include a small (one or two lines) section that states what "Business Needs" are being addressed in the report. The reports will describe performance trends for each performance objective and service levels. The COR and the Contractor will jointly define how to present information for each performance objective. The Contractor may also suggest supporting metrics to be included in the performance reports. The COR and Contractor will agree to the graphical design of reports and frequency of reviews of reports. The monthly Performance Report, at a minimum, will consist of reports on Service Level and Area Metrics described within the b4 [redacted] b4

The Contractor shall provide reporting to convey system configuration information, performance data,

and the status of operational activities. The Contractor shall conduct ongoing analysis of the infrastructure to form the basis for recommendations to maintain and replenish inventory in a manner that enables rapid recovery/provisioning with minimized service disruption and downtime.

1.5 IT SERVICE MANAGEMENT SERVICES

Contractor shall be responsible for providing IT service management for all services. Contractor shall outline how we intend to use industry standards frameworks to support IT service management.

1.5.1 SERVICE CATALOG

Contractor has established and provided a formal service catalog, which describes the MITS and it's features. The service catalog will be used as the reference for MITS delivered by CONTRACTOR and to discuss, provide and manage services provided to CNCS stakeholders and their Contractors.

1.5.2 NETWORK OPERATIONS CENTER

Contractor shall provide 24X7X365 Network Operations Center (NOC) Services. The NOC provides Tier 1 proactive management and incident mitigation for the systems, security and the network. Contractor shall provide fault, configuration, accounting, performance, and security functions (FCAPS) for the network.

Contractor , through the NOC, will perform enterprise infrastructure operations monitoring of all information technology infrastructure components including, but not limited to:

1. Network telecommunications circuits
2. Network switching and routing equipment
3. Network security systems
4. Information technology infrastructure servers (e.g., file, print, domain name service, etc.)
5. Voice over Internet protocol (VoIP) components
6. Video teleconference (VTC) components
7. Video streaming components
8. Environmental monitoring systems
9. Power management devices (e.g., uninterruptable power supply, etc.)

Contractor shall design the monitoring solution to be scalable and dynamic to allow for adding components during the contract period of performance.

Contractor shall initiate proactive repair actions when monitoring identifies potential or existing error conditions. Contractor shall provide recommendations for operational improvements based on trend analysis.

The monitoring application will:

1. Provide automated notifications and alerts
2. Provide a web based management / dashboard interface for Agency IT staff and stakeholders
3. Provide managed device inventory data
4. Provide physical and logical diagrams of managed components
5. Include server and application health and monitoring
6. Support Microsoft Windows Management Instrumentation (WMI)
7. Provide Cisco NetFlow data gathering and analysis or similar capability
8. Support SNMP management of devices using SNMP version 2.
9. Provide Agent and Agentless monitoring
10. Provide server monitoring for industry leading operating systems, RDMS systems, and applications
11. Support industry leading routers and switches, including those manufactured by Cisco
12. Provide monitoring of Cloud Computing platforms used by CNCS
13. Provide capacity planning and monitoring of resources such as memory, CPU, storage, network, and Microsoft Windows Performance Monitor counters.
14. Allow application monitoring for Oracle Database, Oracle Application Server, Microsoft SQL Server, Microsoft Internet Information Server, Apache, Tomcat, World Wide Web, Weblogic, Microsoft Active Directory, Domain Name System, and other custom applications through a scripting interface

15. Identify top applications, conversations, network flows and protocols
16. Provide support for auto-discovery of managed elements
17. Provide monitoring and a complete real time map of the Wide Area Network, to include all network elements like routers, switches, individual links to and from satellite offices

1.5.3 PROGRAM MANAGEMENT AND PROJECT MANAGEMENT

Contractor shall provide the management and functional support needed to manage all aspects of the program. Program and project management activities include: project planning, resource management, quality assurance, risk management, status and problem reporting and administrative support. Additionally, the project manager and the appropriate technical expert will recommend improvements, enhancements and/or changes to the environment, to the appropriate and necessary change management and advisory boards before implementation.

Contractor shall partner with CNCS to ensure that program/project management services identify potential problems, facilitate resolution, and provide outstanding performance in all required business operations, plans and reports. This role will include establishing clear procedures in order to effectively address issues before they become critical problems.

Contractor shall ensure all program, project, or contract management duties performed under this contract are executed in accordance with Project Management Institute (PMI) standards, defined in the Project Management Body of Knowledge (PMBOK) guide. Contractor shall prepare a Project Management Plan describing the technical approach, organizational resources, risk management, communication management and other management controls to be employed to meet the cost, performance and schedule requirements throughout task order execution.

Periodic Task Order Status Reports to include the following information at a minimum:

- Status and progress of tasks
- Cost and schedule variances
- Risks to scheduled deliverables and plans to mitigate them
- Progress against task order service level metrics
- Recommendations for changes or additional activities to ensure that the tasks overall CNCS objectives

Contractor shall:

1. Process and track customer requirements, and manage project implementation
2. Evaluate existing projects/requirements and make recommendations to OIT as to the most advisable approach, assist with processes, architecture diagrams and forms
3. Continue processing and implementing existing projects/requirements.
4. b4 [redacted]
5. Develop and manage an Integrated Schedule with major projects, tracking milestones, and completion dates (e.g., Gantt charts)
6. Plan, schedule, and attend all meetings as required
7. Follow industry best practices, implementing processes to enhance organizational efficiencies, reduce costs, improve IT services, and improve customer satisfaction

All tasks will be performed in a manner consistent with the highest level of professional and technical standards and adhere to industry leading practices such as ITIL, the PMBOK and Capabilities Maturity Model Integration (CMMI) level 2 or higher. All Contractor personnel will be considered fully proficient in the areas in which they work. All Contractor personnel are expected to routinely:

- Keep current with advances in technology and share this knowledge with CNCS OIT

- Act in a consultative manner, proactively searching for creative solutions and strategies
- Respond promptly, professionally and courteously to requests for assistance
- Freely provide knowledge transfer of work products and technology expertise associated with contracted tasks

1.5.4 ENGINEERING SUPPORT

Contractor shall provide engineering support to design and /or trouble shoot computing environment technical issues. Contractor shall ensure all documentation and reference material is updated to match the versions of software, configurations, system functionality, and the operations of the production system.

1.5.4.1 TIER 2- HQ DESKTOP SUPPORT

b4

1.5.4.2 TIER 3- ENGINEERING SERVICES

Contractor shall provide Tier 3 Engineering Services in support of service desk requirements, network related activities, and project management activities that cannot be resolved by Tier 2 service desk technicians. This is final escalation and should be designed to support call ticket/service desk request for service. Network related service will include but not be limited to server specific request, network outages, and limited subject matter expertise. Engineer services will provide staff to support efforts towards the design, configuration, setup, implementation, test and evaluation, subject matter expertise for all IT projects and troubleshooting to isolate the source of, diagnose and/or resolve, or assist in the resolution of IT and telecommunications problems (end-to-end).

1.5.5 REPORTING

Contractor shall provide reports on the full range of services required under this contract to the COR. In addition to progress reporting, Contractor shall inform the designated CNCS Project Managers (PMs) and CORs of any issues, problems and recommendations for the overall efficient accomplishment of the contract and task order goals. Recommendations for actions that need to be taken by CNCS staff, or other Contractors, will be clearly defined and communicated to the responsible CNCS party, and have identified dates for completion.

Contractor shall provide project status reports focused on the successful accomplishment of major milestones/deliverables within the planned schedule and costs. Project reporting will also address any issues, problems, risks or concerns that could negatively impact the project.

Contractor shall provide status reports including self-evaluations and management briefings to document service activities, summarize accomplishments, present analyses of major challenges and offer innovative solutions to improve weaknesses based on established performance measures. The status of all contract deliverables will be monitored with the last revision of the Project Management Plan Reports and presentations will describe achievements, service levels and results in meeting task order objectives.

The Status Report will include:

1. Key accomplishments, completed from last reporting period
2. Issues or key risks, including constraints (e.g., cost, schedule, etc.,) and assumptions, and planned responses for each
3. Stakeholders and systems impacted
4. Tasks planned for next reporting period
5. Anticipated system level changes that require change management (CM)
6. Recommendations and anticipated concerns
7. Roster changes (additions and deletions); and temporary assignments. Roster will include:
    a. Personnel name
    b. Phone number
    c. Email
    d. Duty location
    e. b4 POC for emergency
    f. Duties
8. Open actions for both Contractor and CNCS with due dates and agreed upon priorities (High- impacts schedule if not completed on time; Medium- may impact schedule; Low- needs to be completed but not a critical path item)

1.5.6 CONFIGURATION MANAGEMENT (CM)

b4

1.6 BUSINESS SERVICES

Contractor shall provide services that support CNCS as an organizations and not directly supporting infrastructure services to OIT. These are normally services that support the customer's business processes and facilitate one or more outcomes desired by the customer.

1.6.1 TELEWORK SUPPORT SERVICES

Contractor shall support Agency telework initiatives and provide remote support to Agency staff and Contractors. Agency staff may elect to work from the traditional office environment, from home or telecommuting centers. Agency Field office staff may work at project locations or in support of disaster response initiatives. Limited support will be provided for user home networks. Support may include basic troubleshooting, validating cable and wireless connections, testing IP connectivity and name resolution.

Contractor shall:

Assist teleworking staff with connecting to the Agency network via VPN using Agency and staff owned equipment.

- Provide remote telephone support during business hours for teleworking staff
- Provide basic troubleshooting of home or remote network environments to ensure proper Internet connectivity
- Coordinate GFE distribution, replacement or repair
- Augment support for teleworkers in the event of an Agency declared disaster
- Provide desktop remote control support for Internet attached devices
- Support a "mobile office" platform, including Agency furnished VPN router, wired and wireless LAN components, VoIP telephone station and multi-function printer/fax/scanner.

1.6.2 KNOWLEDGE & DATA MANAGEMENT

Contractor shall develop recommendations for Self Help (Tier 0). The self-help capability will include a searchable knowledge management system that provides users with relevant policy, procedural and administrative documents and knowledge documents encompassing all in-scope hardware and software. This system will provide a knowledge base for technicians and provide self-help for end-users. All data generated, stored, and maintained in the system remains the property of the Government.

1.6.3 ON-LINE SUPPORT PORTAL

Contractor shall provide a secure on-line support portal. The support portal will feature seamless authentication and Active Directory integration for internal Agency staff and Contractors. The portal will provide on-line case status information, new case entry, and access to the Tier 0 knowledge base.

1.6.4 TRAINING

Contractor shall offer on-line, class room, and "brown-bag" training services for Agency staff and Contractors. Contractor shall develop the training curriculum, presentations, materials and learning aids. Training will be provided for desktop and mobile operating systems, GOTS / COTS software applications. All training content will become property of the Agency. Contractor shall provide a cost matrix for training services.

1.6.5 APPLICATION HOSTING

Contractor shall provide computing environments including production and non-production (development and test) capable of hosting all of CNCS applications not hosted by other third party Software as a Service Contractors (example Momentum). Contractor shall manage the applications and their environment to ensure the highest levels of integrity, privacy and availability of the services delivered by those resources.

Contractor shall manage the integration of externally-hosted applications (third party Software as a Service Contractors) with the MITS computing environments ensuring compatibility and performance of the third party application with the MITS infrastructure and delivery of services to the Agency. Contractor shall support the current and future third party services including but not limited to:

- Momentum, the Agency's Financial Management System

- The Agency's personnel system hosted by the United States Department of Agriculture, National Finance Center Bureau of Public Debt Time and Attendance System
- United States Treasury
- Social Security Administration
- Office of Management and Budget
- Microsoft Software as a Service (Office 365, SharePoint, Lync)

1.6.6 APPLICATION/DATABASE MANAGEMENT

Contractor shall provide database administration in support of eSpan, eGrants Classic/eGrants Phase II, AmeriCorps Member, Grantee, and Staff Portals and ARES as well as any future enhancements or development of Agency grant related applications. Contractor shall monitor performance and quality service levels and will proactively address existing or potential issues and plan for any changes to resource demand to maintain or improve expected service levels. Contractor shall maintain the appropriate systems, processes, and tools in place to anticipate and address any security problems and/or breaches, and single points of failure.

Contractor shall perform ongoing maintenance and support for the Agency's applications and their interfaces. Contractor shall:

- Take corrective action necessitated by where the system fails to perform as detailed in SLA's
- Implement requested system modifications in accordance with Agency policies. All modifications must adhere to the Agency's change management processes
- Continuously assess the application set to determine how the system can be made more efficient and effective
- Maintain data and software to the standards necessary to meet or exceed expected service performance and quality levels
- Resolve issues escalated from the Help Desks including evaluating alerts and error messages and taking necessary actions
- Coordinate with network and security teams for any database/Application server related issues
- Revise or produce appropriate documentation
- Perform periodic security testing and annual disaster recovery/failover testing
- Provide ongoing customer support as requested and required
- Support the Agency's reporting and data extraction requirements
- Install and maintain the databases and Application servers (including but not limited to OC4J, MicroStrategy, Visual Crossing, Discoverer, Oracle Reports, Crystal Reports and other reporting tools)
- Implement changes, insertions, deletions, modifications, and extensions to the application set that optimize, improve software performance, maintainability, understandability, efficiency or capacity
- Adapt the application set to adjust to changes that affect its overall operations including but not limited to changes in (1) rules, laws, & regulations; (2) hardware configurations, e.g., distributed processors, load balancing, additional servers , etc.; (3) data formats, file structures; and (4) system software, e.g., operating systems, compilers, utilities, etc
- Institute emergency maintenance in cases where software changes are mandatory to keep the application set operational

1.6.7 DOCUMENT MANAGEMENT SERVICES

Contractor shall host and provide comprehensive management of the existing Indicium DM document management system. This includes, but is not limited to management of access controls, content stores and Microsoft SQL and Oracle database integration. Contractor shall assist the Agency to leverage the capabilities of the Indicium product suite and integration with any other third party products.

b4

[redacted]

Contractor shall comply with all Agency data information handling policies and guidelines and leverage existing Agency technology solutions and associated features to provide data information life cycle management. Contractor shall continually improve data information handling and recommend methods to improve data information handling using the existing system architecture.

1.6.8 WEB SERVICES

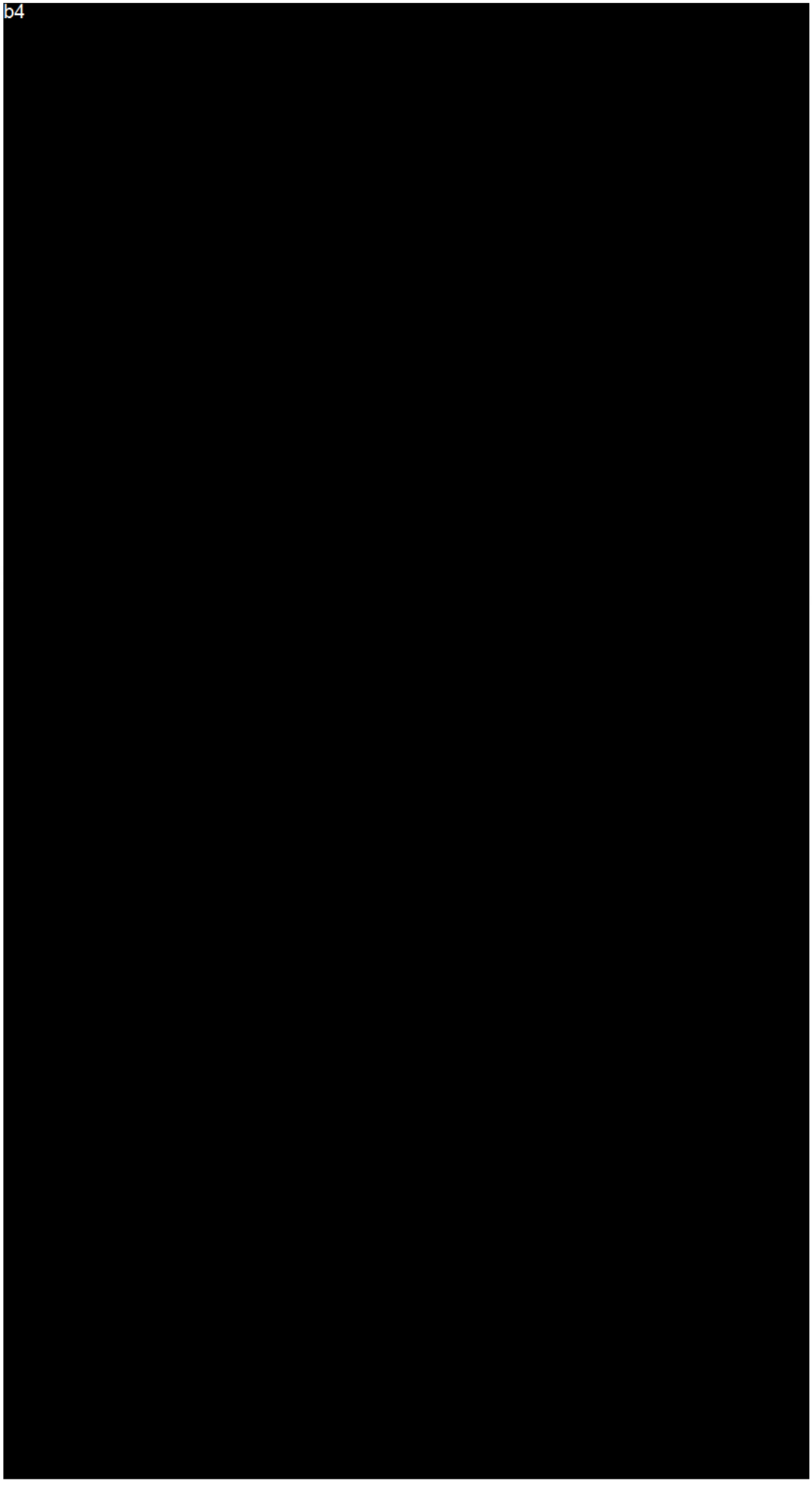
Contractor shall support the CNCS Intranet web sites meeting or exceeding the expected service performance and quality levels. Contractor shall supply technical support to the Web Services team to ensure that the web services are properly supported by the computing environments. Contractor shall provide administrative maintenance and support for the OIT-supported Web based business support software, including calendars, FAQ database and other business software purchased during the life of the Contract. Contractor shall provide support for the OIT's MS SQL database, including routine administrative maintenance and back-up, assisting with analysis of site and answer feedback, and assisting offices with input of new sets of questions and answers; and provide backup and restore services.

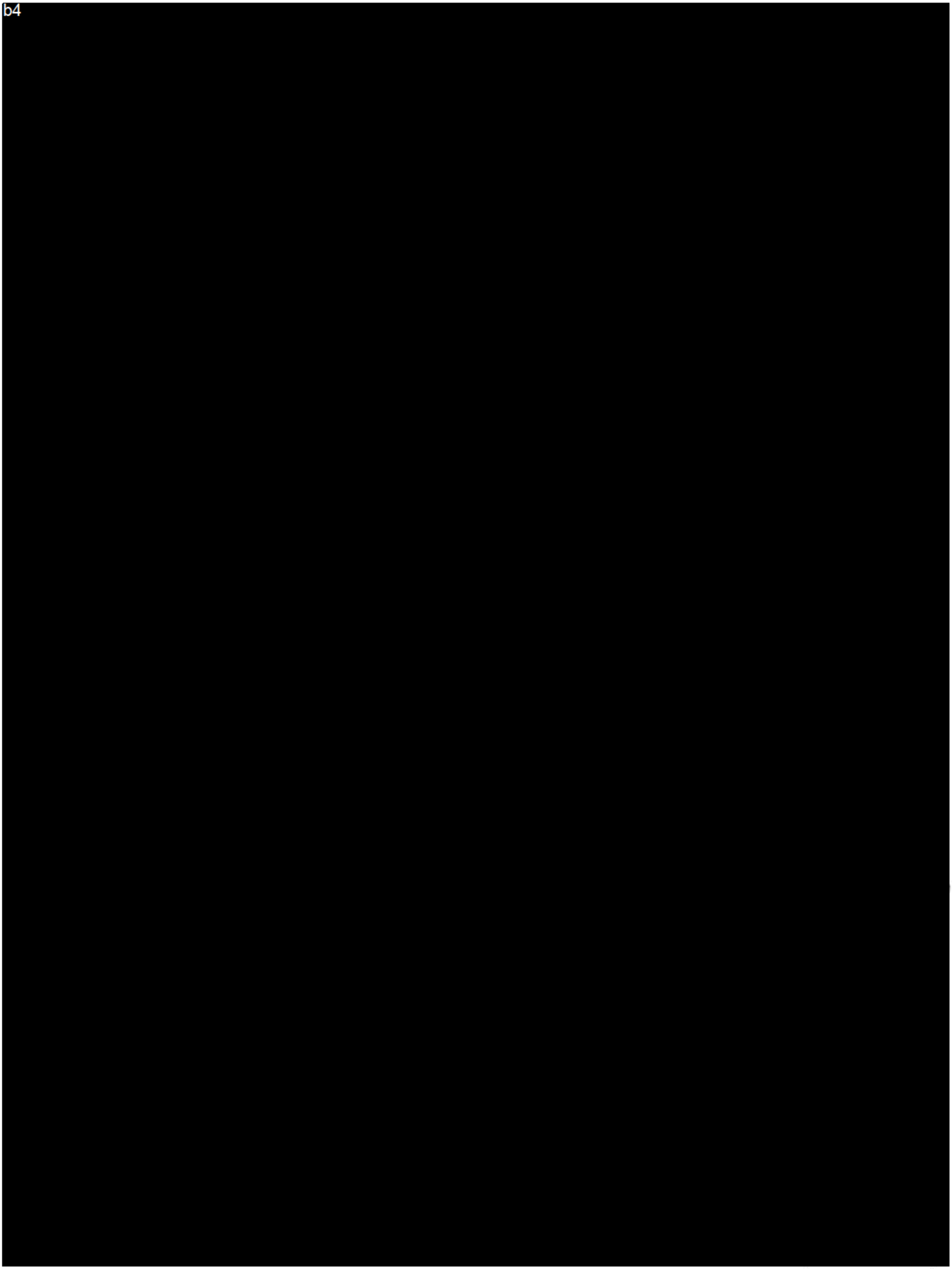
b4

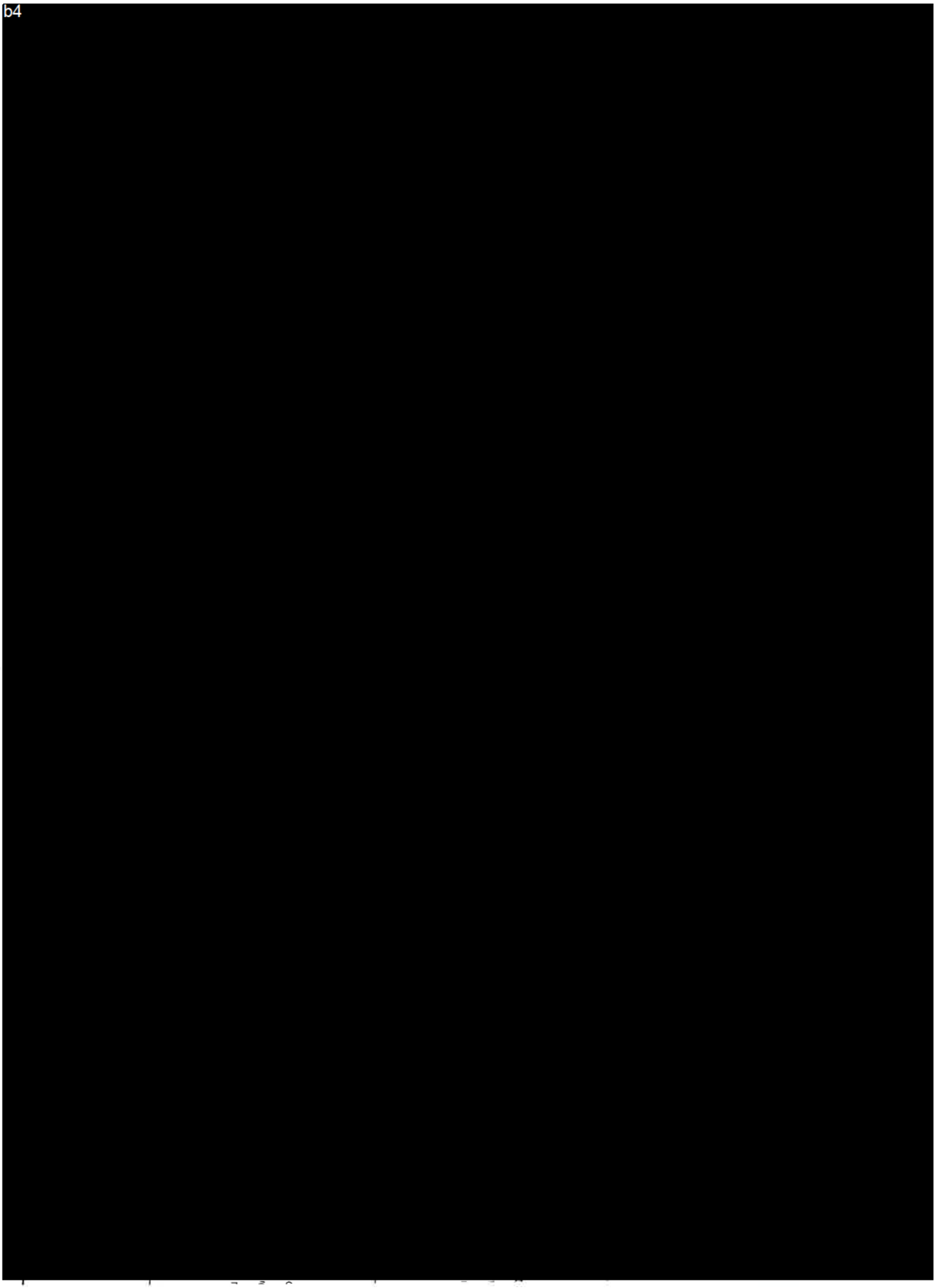
[redacted]

b4

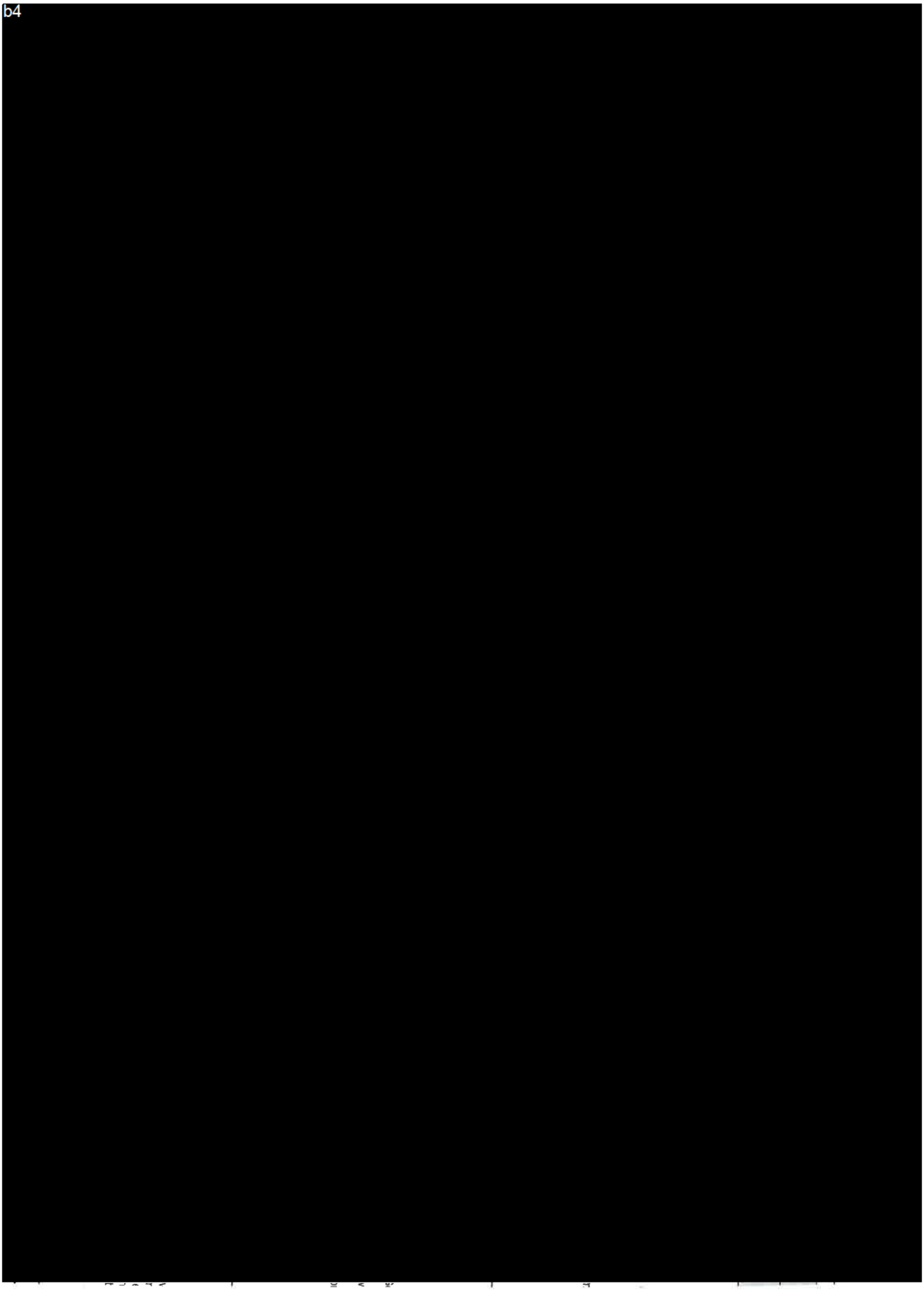
[redacted]


b4

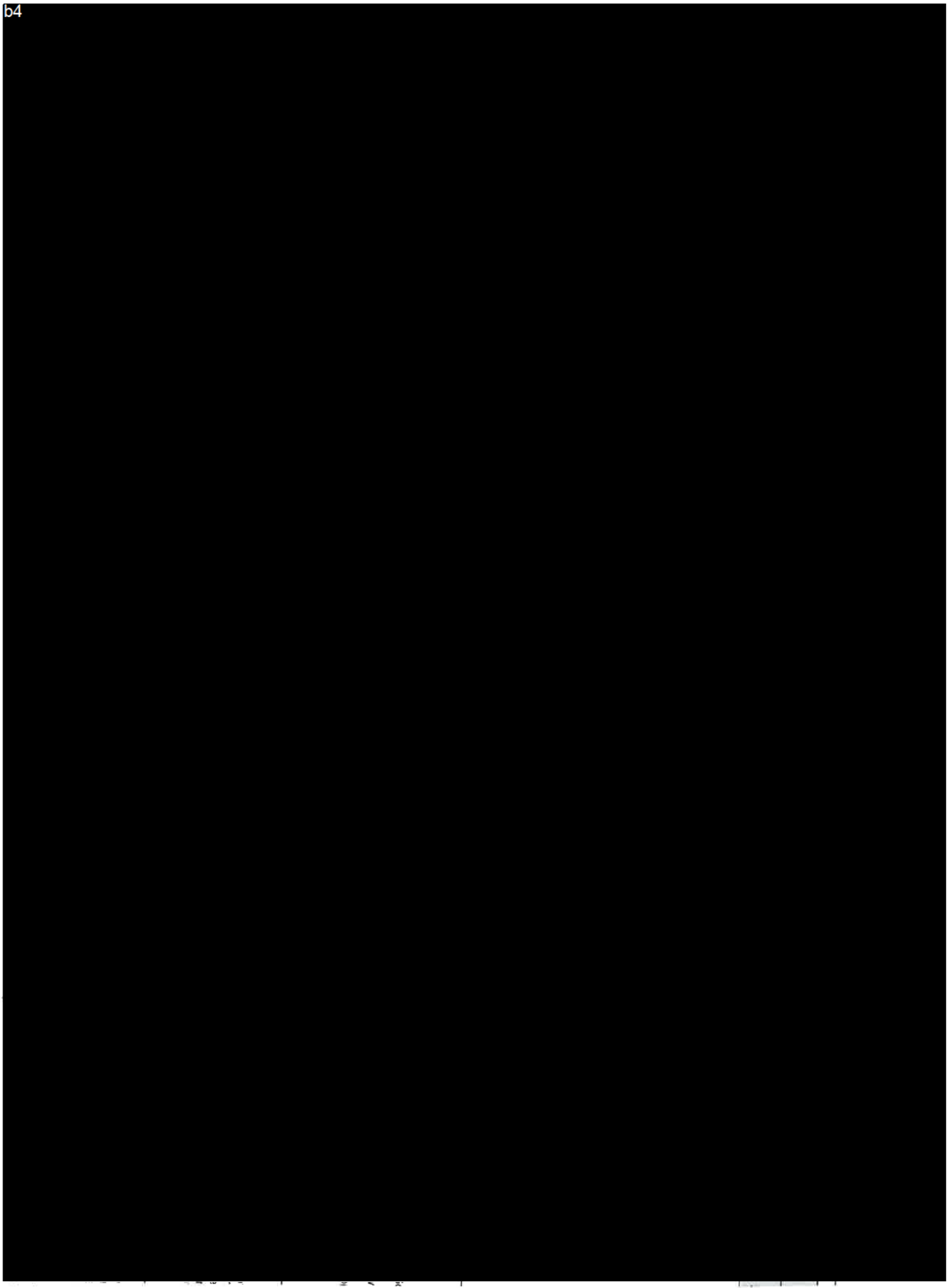

b4

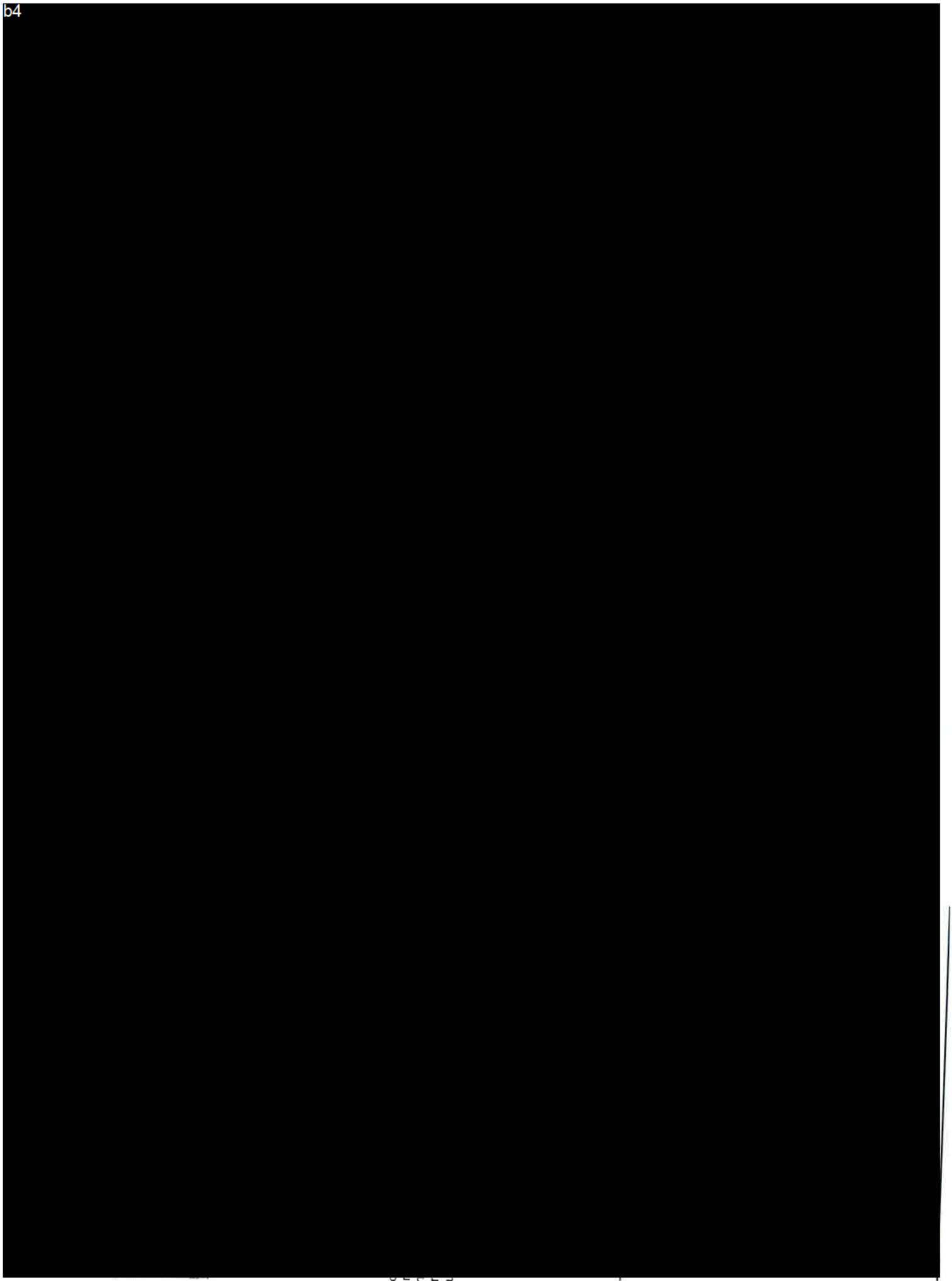

b4

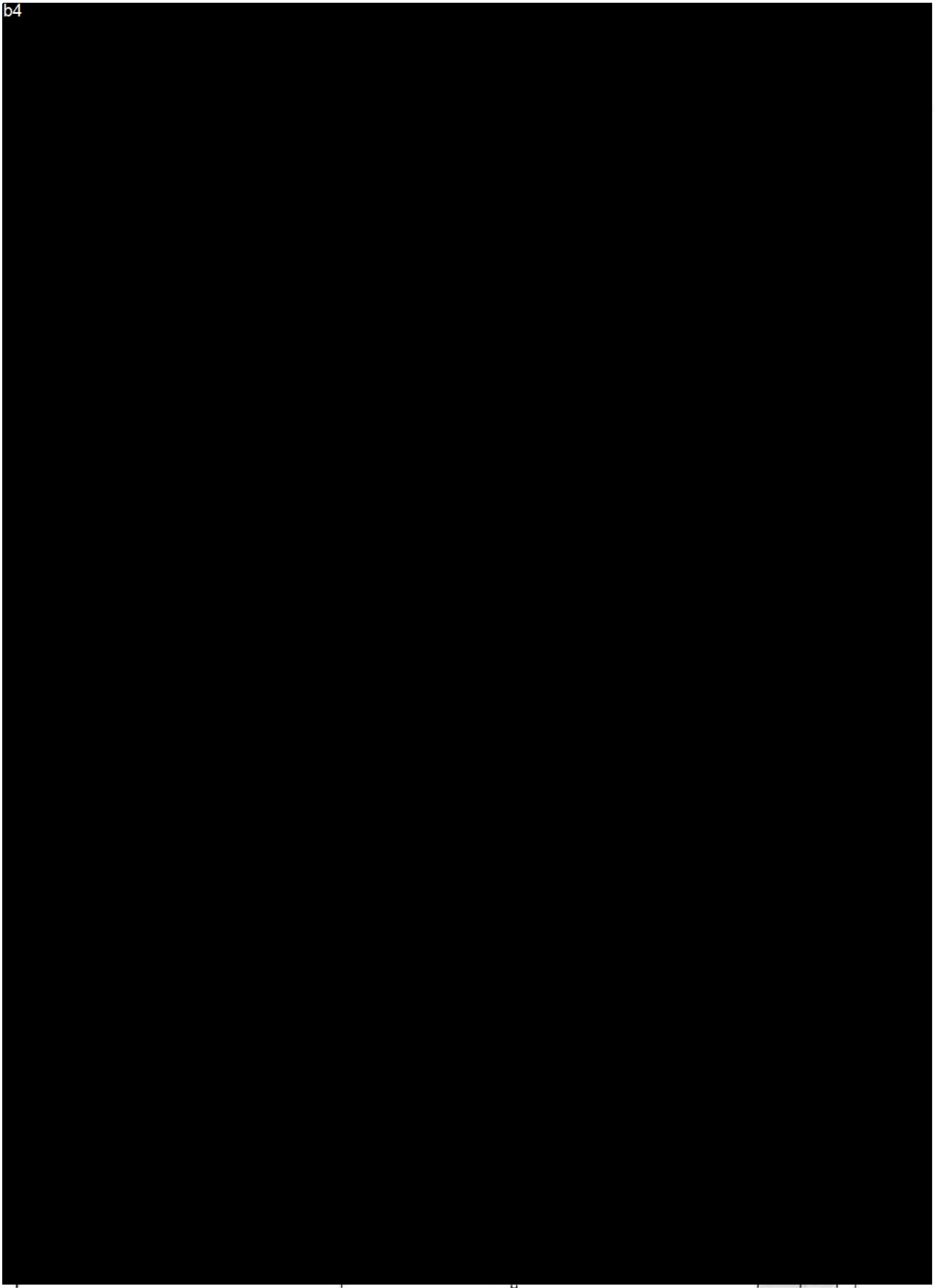
b4


b4

b4


b4


b4


b4

b4

[redacted]