



A PROPOSAL TO

Chicago Teachers' Pension Fund

No. FY23-0009 Network Operations Center "NOC" Managed Services RFP –
Public Version

JUNE 30, 2023



SSAE 16 SOC 2, Type II Attestation

Standing at the apex of Sentinel’s myriad awards, honors and certifications is its SSAE 16 Service Organization Control (SOC) 2, Type II Attestation which has been undertaken annually by the nationally-renowned auditing firm Plante Moran, PLLC for the past three years. The SOC 2, Type II attestation is the highest and most rigorous in the SSAE 16 portfolio of audits, evaluating Controls and Processes that encompass the Five Trust Service Principles of Security, Availability, Processing Integrity, Confidentiality and Privacy.

Why should this matter to you? The SSAE 16 attestation provides independent validation and assurance that Sentinel is in compliance with best practices regarding items of critical importance to you -- security, confidentiality, data protection, project management and IT strategic solutions, to name a few. If you are seeking consulting or services support for your IT environment, the SOC 2, Type II attestation should be one of the most important factors in your evaluation.



The SSAE 16 Attestation is a standard that was created by the American Institute of Certified Public Accountants (AICPA) in 2010 to replace the SAS 70 certification process, and expand reporting to the effectiveness of a service organization’s controls relating to operations and compliance.

A. Cover Letter

- a. In a brief statement please identify the work requested in this RFP accompanied by the supporting reasons why the Respondent believes it is qualified to perform the engagement. The letter should be signed by the Respondent's representative authorized to contract on behalf of the Respondent.

Sentinel Response:

Lupe Garcia, Counsel
Sandy McNamara, Paralegal and Contract/Procurement Analyst
425 S. Financial Suite 1400
Chicago, IL 60605

Dear CTPF Review Committee:

Enclosed, please find Sentinel's response to Chicago Teachers' Pension Fund Request for Proposal Specification No. FY2023-0009, Network Operations Center "NOC" Managed Services.

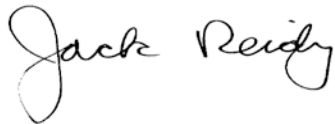
Sentinel's vast background in managed services and our insight into the CTPF network provides us with a compelling story to continue providing NOC services to the Fund. We appreciate the opportunity to offer our services, and look forward to discussing our response with you in greater detail.

Sentinel has enjoyed a positive, professional working relationship with CTPF since 2016. Throughout our time of service to CTPF, we have continuously sought to improve the delivery of our service and reduce costs whenever possible. We look forward to continuing to provide exceptional service to the Chicago Teachers Pension Fund in the future.

Sentinel prides itself at servicing some of the largest, most prestigious organizations within the United States. Our success is directly attributed to our ability to design and implement technology solutions utilizing Sentinel's vast personnel and expertise to meet and exceed our customer's expectations. Sentinel's methodology, along with our singular focus, to provide the most comprehensive price/performance solution in the industry, are the paramount reasons for our success.

For the reasons cited above, Sentinel believes that we are best positioned to be a preferred vendor for this engagement.

Sincerely:



Jack Reidy
Senior Sales Executive
630-769-4325 Phone
jreidy@sentinel.com

B. Title Page

a. Date

Sentinel Response: June 30, 2023

b. Subject

Sentinel Response: Network Operations Center “NOC” Managed Services.

c. Respondent’s name and chief executive officer (or the equivalent)

Sentinel Response: Sentinel Technologies, Inc.
Robert Lenartowicz, Co-President/Chief Operations Officer
Brian Osborne, Co-President/Chief Sales and Marketing Officer
Tim Hill, Co-President/Chief Financial Officer

d. Respondent’s address

Sentinel Response: 2550 Warrenville Road, Downers Grove, IL 60515

e. Respondent’s website address

Sentinel Response: www.sentinel.com

f. Respondent’s phone number

Sentinel Response: 630.769.4300

g. Respondent’s fax number

Sentinel Response: 630.769.1399

h. Contact’s name

Sentinel Response: Jack Reidy

i. Contact’s title

Sentinel Response: Senior Sales Executive

j. Contact’s phone number

Sentinel Response: 630.769.4325

k. Contact’s email address

Sentinel Response: jreidy@sentinel.com

TABLE OF CONTENTS

C. Table of Contents

SSAE 16 SOC 2, TYPE II ATTESTATION.....2

A. COVER LETTER.....3

B. TITLE PAGE.....4

C. TABLE OF CONTENTS.....5

D. PROJECT PLAN.....6

E. BILLING8
Pricing 8

F. FIRM’S BACKGROUND, QUALIFICATIONS, AND EXPERIENCE.....9

G. INSURANCE, LIABILITY, CONFIDENTIALITY, AND LITIGATION 13

H. CONTRACT OR AGREEMENT MANDATORY CTPF TERMS..... 16

I. REFERENCES..... 17

J. REQUIRED DISCLOSURES..... 19

K. EXHIBITS AND ATTACHMENTS 23

Exhibit I: Sample – Managed Services Scope of Work 24

Exhibit II: Additional Deliverables or Services 35

Exhibit III: Ownership Structure 73

Exhibit IV: Resumes 74

Exhibit V: Pre-Employment Screening Services 80

Exhibit VI: Sample Incident Response Agreement 84

Exhibit VII: Sample Certificate of Insurance 87

Exhibit VIII: Inventory 88

D. Project Plan

a. Address the various tasks, services, and deliverables outlined in Section III. Scope of Work and describe the specific approach that will be taken in performing each task or service or providing each deliverable.

Section III: Scope of NOC Managed Services:

1. Continuous and uninterrupted network operations service and support

- Monitor, analyze, alert, troubleshoot, diagnose, and report on the status and health of specified network equipment and appliances as well as telecommunication services
- Monitor, analyze, alert, and report on KPI's for power, cooling, and ambient temperature and humidity using existing monitoring equipment
- Monitor, analyze, alert, and report on wireless KPI's including AP connections to controllers, client traffic volume, signal strength and interference
- Monitor, analyze, alert, and report on routing and switching KPI's including stability of neighbor connections, paths, and Internet connectivity
- Monitor, analyze, alert, and report on network traffic KPI's for packet drops, endpoint latency, and application availability
- Respond to specific monitored events following approved customer notification and action procedures
- Provide Fund IT staff access to monitoring dashboards and ticketing and documentation portals used by the NOC

2. Maintain Cisco equipment and services as needed.

- Prepare Cisco SMARTnet licensing renewals.
- Perform approved, scheduled firmware, software, and hardware updates and upgrades on Cisco hardware including firewalls, routers, switches, and security appliances.
- Provide on-call support when needed for performing Cisco maintenance and upgrade work
- Introduce enhancements through deploying new features related to update and upgrade work
- Review and update procedure documentation and network diagrams after performing upgrade work

3. Health checks and status reporting

- Perform routine equipment and service health checks
- Report on NOC management KPI's including for volume of trouble tickets, mean time to respond, mean time to resolve, and event management
- Conduct QBR (Quarterly Business Review) assessments to analyze activity summaries and evaluate the provided level of quality assurance

Sentinel Response: See *Exhibit I* for Managed Services Scope of Work.

b. Describe how Respondent has the necessary dedicated staffing and bandwidth to take on this engagement.

Sentinel Response: Sentinel currently has over 150 technical engineers on staff 24x7x365 that are separated into the following technology stacks:

- Enterprise Networking
- Data Center/Virtualization
- Voice and Collaboration
- End User Support
- Customer Service

So depending on where cases are being generated in your environment, it will be a combination of those teams coming together to ensure we resolve any issues that may arise.

c. Describe any deliverables or services, not included in Section III. Scope of Work that your Firm would suggest be provided in order to provide more complete and thorough services.

Sentinel Response: Please see *Exhibit II: Additional Deliverables or Services*.

d. Indicate the location of the office(s) from which the work on this engagement is to be performed.

Sentinel Response: Sentinel Technologies' headquarters are at 2550 Warrenville Rd. in Downers Grove. Sentinel's NOC is located at the same facility and is operated 24x7x365 days a year with "live" personnel

e. Provide a percentage break down of how much of the engagement will be performed on your site, CTPF's site or remotely.

Sentinel Response: 100% of the work discussed in this response will be performed remotely by Sentinel engineers. Sentinel does offer onsite services, but those services fall outside of the proposed scope of work listed in this RFP response.

f. Identify tasks that will be performed by your Firm and tasks that will be performed by CTPF's staff.

Sentinel Response: Sentinel engineers will perform all tasks/actions necessary within the scope of work for devices covered under the Managed Services agreement. Things that would fall outside of the scope of work for devices covered under managed services can either be performed at a time and materials rate or scoped out as a project (i.e., Major software upgrades, security breaches, hardware maintenance, etc.).

BILLING

E. Billing

a. State any special considerations with respect to billing or payment of fees and expenses that Respondent offers and that you believe would differentiate your Firm from other proposals and make your Firm’s services more cost effective to the Fund.

Sentinel Response: Sentinel offers prepaid discounts for managed services on an annual or multi-year basis. We can discuss this in more detail if CTPF is interested in our prepayment programs.

b. CTPF expects the lowest rate charged by Respondent for its governmental and nonprofit clients. If for any reason Respondent is unwilling or unable to charge the lowest rate, please explain why.

Sentinel Response: Sentinel will comply.

c. The billing rate will be fixed for the term of this engagement.

Sentinel Response: Sentinel will comply.

Pricing

SUMMARY				
One Time Setup			\$0	
Monthly Total			\$2376.40	
SENTINEL MANAGED SERVICES				
<u>INFRASTRUCTURE</u>				
<i>Product</i>	<i>Location</i>	<i>Quantity</i>	<i>Discounted Unit Cost</i>	<i>Comments</i>
WAN Routers-Voice Gateway		2	\$66.00	
Firewall Security Device		3	\$176.00	(2) Firepower, (1) FMC
Switch		12	\$35.20	
Wireless Access Point		20	\$4.40	
Wireless Controller		2	\$132.00	
<u>PROACTIVE MONITORING</u>				
<i>Product</i>	<i>Location</i>	<i>Quantity</i>	<i>Discounted Unit Cost</i>	<i>Comments</i>
NOC Monitoring + Alerting - Network/UPS		5	\$17.60	Avtech, Liebert, APC
<u>SERVERS & VIRTUALIZATION</u>				
<i>Product</i>	<i>Location</i>	<i>Quantity</i>	<i>Discounted Unit Cost</i>	<i>Comments</i>
Application Server OS Only		4	\$176.00	Linux Web Servers
<u>SUPPORT SERVICES</u>				
<i>Product</i>	<i>Location</i>	<i>Quantity</i>	<i>Discounted Unit Cost</i>	<i>Comments</i>
Service Fee		1	\$150.00	

Confidential Information, property of Sentinel Technologies, Inc.

F. Firm's Background, Qualifications, and Experience

a. Briefly describe Respondent's background, history, and ownership structure, including any parent, affiliated or subsidiary company, and any business partners. The firm must be regularly-established in the industry of providing the services outlined in Section III. Scope of Work, and have experienced personnel able to provide the required services. CTPF may request information substantiating the above requirements. Failure to provide this information may result in a Respondent's proposal being declared non-responsive.

Sentinel Response: For more than 40 years, Sentinel has been recognized as a top-tier business technology solutions and services provider dedicated to delivering the highest quality Customer service and support. Even as our services have spanned generations of technology, Sentinel has stayed at the forefront of IT developments and maintained a singular focus on providing practical and innovative solutions. With single-source accountability, Sentinel's proven repeatable methodology, processes and experienced teams can efficiently address a full range of IT needs - from NOC monitoring and managed services, to communications, to data center, to cloud solutions, to business process improvement and assessments, to targeted applications and end-to-end IT solutions. Our proven success has allowed us to expand from our original charter of providing technology maintenance services to our current standing as one of the leading IT services and solutions providers in the U.S. and beyond. Sentinel's engineers, Customer Service and support, and project management team's reputation has become synonymous with high quality, cost effective solutions for our customers. Sentinel's pricing response will reflect our sincere desire to establish a long-term partnership. Sentinel is confident we will emerge as the top option for executing your business critical managed services, but also as your preferred partner for contributing to your overall growth and future success.

Sentinel provides our customers with the complete solution: vision, design, product, implementation, documentation, service and support. Sentinel's services span the range of business verticals in the mid-market, upper mid-market, and enterprise level organizations. Companies in Financial and Banking, Healthcare, Government, Education, Legal, Utilities, and Manufacturing verticals have all taken advantage of Sentinel's ability to take either full responsibility or act as a supplemental contributor to our customer's most important business technology initiatives.

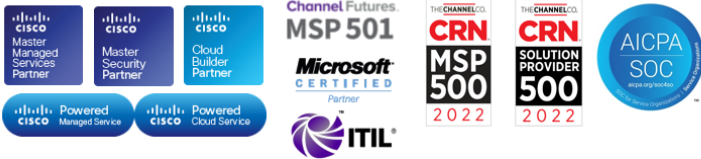
Headquartered in Downers Grove, IL, Sentinel Technologies has independently managed offices in nine locations: Chicago, IL, Springfield, IL, Milwaukee, WI, Phoenix, AZ, Detroit, MI, Grand Rapids, MI, Lansing, MI, Fort Lauderdale, FL and Denver, CO, allowing us to service our customers both nationally and internationally. Sentinel applies an extraordinary breadth of technical solution expertise to design, sell, deploy and support our customer's business technology needs. Our unwavering commitment to thought leadership and customer satisfaction maximizes both the value of technology investments and its impact to the business. When it comes to achieving a tangible ROI and sustainable performance from your IT environment, Sentinel stands apart. Sentinel's large service staff (650+ employees), multitude of original equipment manufacturers (OEM) certifications, a 24x7 Customer Care Center and a professionalism and commitment to service excellence act in combination to ensure a successful partnership.

The Sentinel Difference

Qualifications & Capabilities

Sentinel Partnership Recognition & Awards

- Channel Futures MSP 501 Worldwide Company Ranking #17
- World's Top 501 Managed Service Providers by MSPmentor
- MSP & Solution Provider 500 by CRN
- Top MSP Recognition by Schneider Electric
- Cisco Masters for Managed Services
- Cisco Masters for Security
- Cisco Masters for Cloud Builder & Services
- AWS Partner Network (APN) Advanced Consulting Partner
- AWS Certified Managed Security Service Provider (MSSP)
- Cybersecurity Excellence Gold Awards in 2022 (Gold Winner in 11 Categories)
- Meraki Managed Service Partner
- Dell EMC Premier Partner
- VMware Solution Provider Enterprise Partner
- First Global Cloud Provider to Achieve Cisco Security as a Service Designation
- Cisco Channel Customer Satisfaction Excellence



With over 14,000+ Technical Skills & 2400+ Certifications (Across Various Vendor Partners)

2,750+	10
1,940+	545
114	139
220+	658
403	70
27	10
27	12

Sentinel Alliances & Partnerships

Enterprise Network Portfolio								
Collaboration Portfolio								
Data Center & Cloud Portfolio								
Cyber Security Portfolio								

Please see Exhibit III Ownership Structure.

FIRM'S BACKGROUND, QUALIFICATIONS, AND EXPERIENCE

b. Provide the size of the Firm including number of offices and number of full-time employees. Identify the key personnel proposed for the CTPF engagement, emphasizing specific experience on contracts similar in scope to the requirements of this RFP. Describe his or her position, current responsibilities, areas of expertise, experience, education, professional designations, and memberships. Include details regarding the proposed management of the personnel who would be assigned to the CTPF engagement. CTPF expects a reasonable notice of key personnel being removed from the engagement and reserves the right to approve the replacement of key personnel.

Sentinel Response:

Frank Lopez	Diane Jackson	Joshua Marcus	Jack Reidy	Scott Sibberson
Quality Assurance & Onboarding	Managed Services & Support Solutions	Managed Services & Support Solutions	Chicago Teachers' Pension Fund Account Manager	Support Solutions
Managed Services & Cloud	Product Manager	Solutions Architect	Sales Executive	Support Services Manager
Director of QA & Onboarding				

Customer Success Manager – Dawn Greene	24x7x365 Network Operations Center (NOC) – 150+ engineers and growing
--	---

Jack Reidy, Sales & Account Manager, will be dedicated to Chicago Teachers' Pension Fund. Jack Reidy will act as the primary point of contact across all aspects of the relationship. As the dedicated Account Manager, Jack Reidy will be involved in all sales activities, post sales activities, ongoing projects, status meetings, onboarding meetings, escalations, and all other applicable responsibilities requested by Chicago Teachers' Pension Fund. Chicago Teachers' Pension Fund will have access to all key members for any request or support.

Please see *Exhibit IV* for resumes.

c. Provide the number of years that the Firm and any identified individuals have been providing the services requested in this RFP.

Sentinel Response: Sentinel's managed services practice has been supporting customers for 20+ years.

d. Provide details on your Firm's employee benefit industry experience/expertise.

Sentinel Response: Sentinel's HR department partners with leaders in the benefits industry to provide our employees with cutting edge benefits.

e. Indicate the number and nature of part-time professional staff to be employed in this engagement.

Sentinel Response: Sentinel's 24x7x365 support team that consists of 150 full-time technical engineers will be supporting this engagement.

FIRM'S BACKGROUND, QUALIFICATIONS, AND EXPERIENCE

f. Will your Firm use outside contractors (subcontractors) for this engagement? If so, what confidentiality agreement is in place to protect sensitive information from disclosure? What allocation of the scope of services will be assigned to outside contractors (subcontractors)?

Sentinel Response: Sentinel will not be using subcontractors for the services provided in this RFP.

g. Indicate Respondent's due diligence process in hiring, evaluating, and monitoring its staff and contractors, as applicable.

Sentinel Response: Please see *Exhibit V: Pre-Employment Screening Services*.

h. List any known professional or personal relationships Respondent or its employees or contractors may have with individual CTPF Board members and/or Fund staff.

Sentinel Response: None

i. Identify any potential or actual conflicts of interest you have in providing services to CTPF. State whether you have ever provided services to CTPF, the City of Chicago, the Chicago Board of Education ("Chicago Public Schools" or "CPS"), the Chicago Teachers' Union ("CTU"), the Retired Teachers' Association of Chicago ("RTAC"), the Chicago Principals and Administrators Association ("CPAA"), any Chicago charter school, or any employee group or trade organization related to the aforementioned entities. If so, please state the name of each such client or former client, contact information, and the nature and time frame of such representation. In providing such information you consent to and agree to release CTPF from any liability that may result from contacting such client(s) and communicating with such client(s) about your prior engagements, and soliciting an opinion regarding the work performed for such reference. In addition, please state how you intend to resolve any potential or actual conflict of interest.

Sentinel Response: None

j. Identify all public sector or ERISA fund clients who have terminated their working relationship with you in the past five (5) years and provide a brief statement of the reason(s) for the termination. Provide each client's contact information. You consent to and hereby release CTPF from any liability that may arise from contacting your former client(s) and communicating with them about the work you performed and the reason for your termination.

Sentinel Response: None

G. Insurance, Liability, Confidentiality, and Litigation

a. What assurances can you provide that your Firm will not be subject to cyberattacks? Describe security and protection measures and provide copies of any and all related policies.

Sentinel Response: There are no 100% fool proof plans regarding security and cyber attacks. It is a constant and never ending aspect of protecting your network and brand. Notwithstanding, Sentinel implements layer upon layer of security measures to deter potential “hacks”. In addition, as a Security Service provider, we get audited annually and we perform penetration tests on our network semi-annually.

b. Describe your expected response time to notify us if a cyber-attack or security breach should occur and the actions you would take to mitigate damages.

Sentinel Response: We will notify any affected customer of a cyberattack as soon as possible, or at least 72 hours from discovery. We have an experienced in house incident response team that will expeditiously mitigate damages. Please see *Exhibit VI* for Sample Incident Response Agreement.

c. Please describe the levels of your professional liability insurance coverage for client security breaches (cyber risk) and any fiduciary or professional liability insurance your Firm carries. Is the coverage on a per client basis or is the dollar figure applied to the Firm as a whole? List the insurance carriers.

Sentinel Response: Please see *Exhibit VII: Sample Certificate of Insurance*.

i. What limitation on liability, if any, do you impose through your contract? The Firm must not seek to unreasonably limit their liability for negligence.

Sentinel Response: We limit liability for consequential or incidental damages, with the exception of gross negligence or willful misconduct.

ii. Are you bonded?

Sentinel Response: We do have a performance bond company through which we can obtain a bond if needed.

iii. Does coverage for liability, due to your negligence, continue for a period following termination of the contract? If so, for how long?

Sentinel Response: Yes, please see *Exhibit VII: Sample Certificate of Insurance*.

iv. Identify the amount, type of coverage, deductible, and any coinsurance.

Sentinel Response: Please see *Exhibit VII: Sample Certificate of Insurance*

d. It is expected that the selected firm will have adequate quality control procedures in place to guarantee the accuracy of the work performed. Please describe your quality assurance procedures.

Sentinel Response: Sentinel has a Quality Control team in place to ensure that our clients and employees have resources that they can go to for service delivery. For our clients, this may involve monthly and/or quarterly meetings to discuss current service level agreements, ticket resolution, ticket response times, etc. The goal of the meeting is to do a “synch check” with our clients so that the contracted agreements align with the service deliverables. Below is a workflow that our Quality Control team follows:

- Notification of Customer Concern
 - Email is sent to QualityCounts@sentinel.com indicating customer is experiencing a Quality Assurance issue.
 - Customer creates a ticket and marks it with the Equipment Type of “Quality Assurance” or notates in Problem Title/Description that this is a “Quality Assurance” issue.
 - Sentinel Customer Service routes ticket to QA Team.
- QA Team Engaged and Ticket Created.
 - QA team reviews the customer concern, assigns the issue a QA category and works with Customer Service to **open ticket under the customer’s account**.
 - If ticket was already created directly by the customer then QA team works with Customer Service to update ticket so it indicates the QA category.
 - QA team emails customer acknowledging they are working on the issue and providing the ticket number in case of customer follow up.
- QA Team Reviews Issue and Documents Ticket.
 - Issue is investigated and notes added to ticket. All notes will be clear and concise as they will potentially be customer facing.
 - Ticket resolution notes will indicate:
 - Immediate actions taken to resolve customer issue.
 - Lessons learned and any changes made to prevent issue in the future.
- QA Formal Documentation
 - Formal documentation is completed and document is emailed to customer and appended to ticket.
- Follow up and Ticket Closure
 - If customer has any additional follow up items, the QA Team will review and respond before closing out the QA Ticket.

e. Provide the last 2 years of SOC 1 and SOC 2 type II reports or respond with N/A if you do not have such reports.

Sentinel Response: We can provide the last two SOC 2 reports upon award.

f. What is the organization's policy on confidentiality during and after the engagement?

Sentinel Response: Sentinel has strict standards on confidentiality. We are audited and follow compliance standards for handling our client's information.

g. Has your Firm ever been involved in a lawsuit in the last ten (10) years involving any services provided by the Firm?

Sentinel Response: None

h. If so, provide details, including description of the lawsuit, dates, and outcomes including any filed claims that were settled without litigation. Has your Firm, related entities, affiliates, principals, and/or officers been a party in any material civil or criminal litigation, or subject to investigation, disciplinary action, or regulatory review, whether or not directly related to services requested by this RFP? If so, provide details, including dates and outcomes.

Sentinel Response: None

i. If yes, please provide details, including dates and outcomes.

Sentinel Response: None

i. Describe any anticipated litigation in which your Firm may be involved.

Sentinel Response: None

ii. Describe any anticipated litigation in which your Firm may be involved.

Sentinel Response: None

H. Contract or Agreement Mandatory CTPF Terms.

a. Please state Respondent's exceptions to the below CTPF terms for negotiation purposes.

Sentinel Response: No exceptions; it is our understanding that a contract is to be negotiated after award.

b. Provide additional details, if any, that we should be aware of regarding your contracting process.

Sentinel Response: Sentinel has worked with CTPF for many years negotiating contracts and we are quite familiar with the requirements and approval process.

i. The resolution of all dispute(s) arising from a contract award shall take place in the State of Illinois, County of Cook.

Sentinel Response: Agreed.

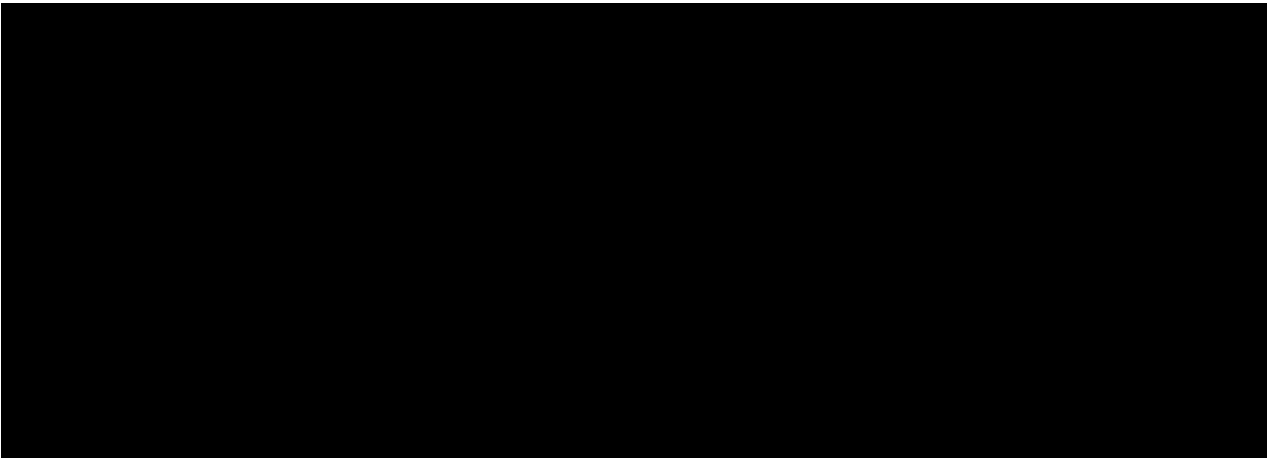
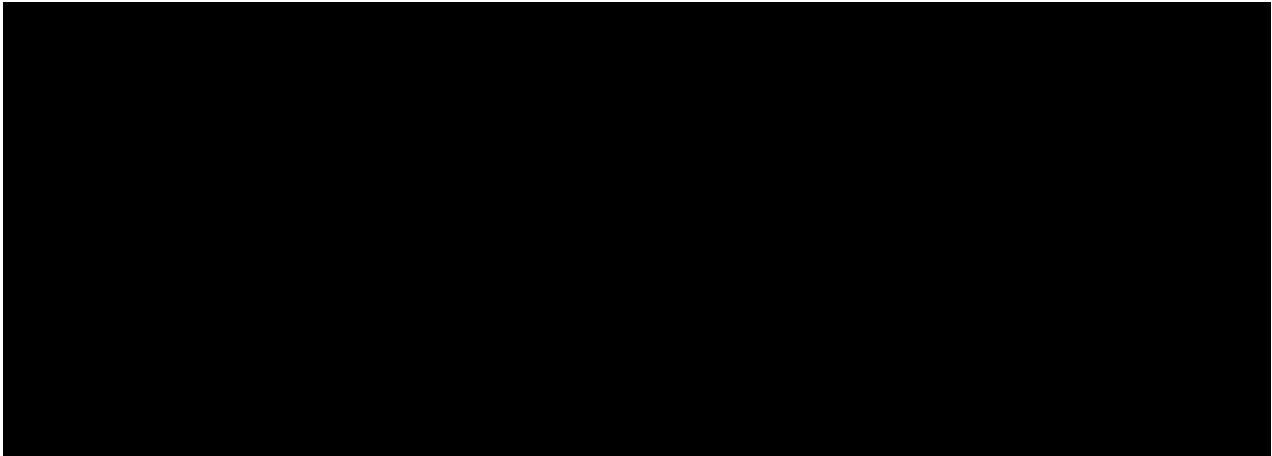
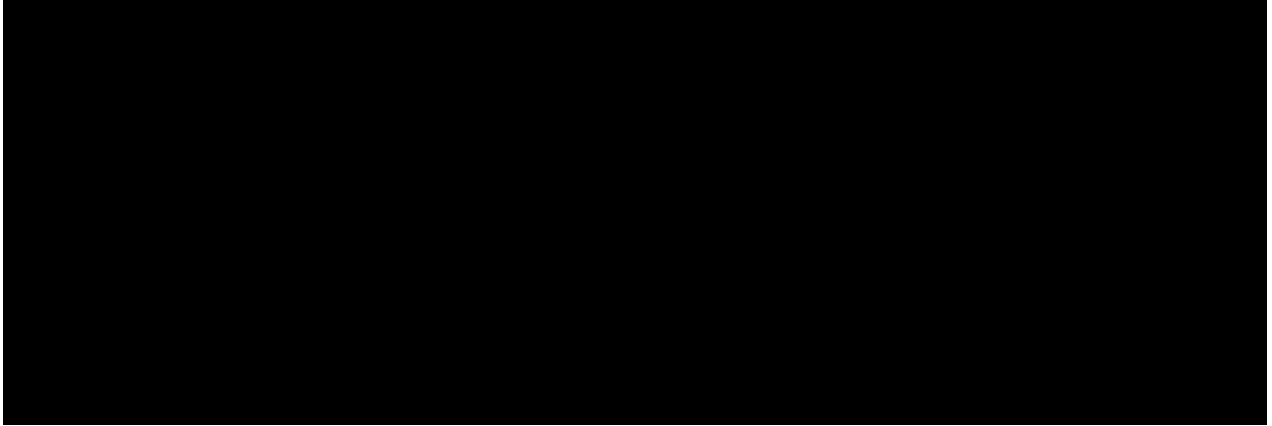
ii. CTPF shall not waive its right to a Jury Trial.

Sentinel Response: Understood.

I. References

a. Please provide three (3) references who are clients for whom you have performed work similar to that requested in this RFP. Include the reference name, title, entity, address, telephone number, and description of the services provided.

Sentinel Response:



REFERENCES

b. In providing such information, you consent to and hereby release CTPF from any liability that may arise from contacting your references and communicating with such references about your prior engagements, and soliciting an opinion regarding the work performed for such reference.

Sentinel Response: Sentinel would like to know the timeframe that direct contact will be made with our clients. This will allow us to reach out to them and let them know that a third party will be contacting them about services that we render.

In addition to the references above, Sentinel has been providing managed services to CTPF for the past 5 years and Dan Oakes can provide feedback on our offering to the review Board

J. Required Disclosures

a. **All Respondents must provide answers to each written disclosure requested below in categories (i) through (ix) as part of their RFP response.** Note that VIII(J)(a)(vi) below requires completion of the EEOC chart attachment to this RFP. **Failure to provide answers to each disclosure question or failure to provide the completed EEOC chart may cause your proposal to be deemed non-responsive.** Respondents should use “none” or “not applicable” as appropriate, but a response **must** be provided for each disclosure category below. Your disclosures must be clearly labeled as “J. Required Disclosures.”

Sentinel Response: Understood.

(i) The Respondent must disclose, labeling each category, separately: (a) any entity that is a parent of, or owns a controlling interest in, the Respondent, (b) any entity that is a subsidiary of, or in which a controlling interest is owned by, the Respondent, (c) any persons or entities who have an ownership or distributive income share in the Respondent that is in excess of seven and one-half percent (7.5%), and (d) any persons who serve as executive officers of the Respondent, including their titles.

Sentinel Response: Please see Exhibit III: Company Ownership.

(ii) The Respondent must disclose, separately: (a) any direct or indirect payments in excess of \$1,000 per calendar year within the prior five (5) calendar years made to any community or not-for-profit organization relating to public education by: (i) the Respondent, (ii) any executive officer of the Respondent, (iii) any parent entity of the Respondent, (iv) the executive officers of any entity that is a parent of, or owns a controlling interest in, the Respondent, and (v) any Shareholder of Respondent with ownership or a distributive income share in the Respondent that is in excess of seven and one-half percent (7.5%); (b) any formal involvement with any community or not-for-profit organization relating to public education by any person or entity identified in (a) above; and (c) any involvement as a member or director of a charter school that contributes to the Fund of any person or entity identified in (a) above. For purposes of this Section VIII(J)(a)(ii) and (iii), “Shareholder” shall mean any person who has an ownership or distributive income share in the Respondent.

Sentinel Response: None.

(iii) The Respondent must disclose if: (a)(i) any executive officer of the Respondent, (ii) any parent entity, (iii) the executive officers of any entity that is a parent of, or owns a controlling interest in, the Respondent, and (iv) any Shareholder of the Respondent with ownership or a distributive income share in the Respondent that is in excess of seven and one-half percent (7.5%) has given any direct or indirect financial support in excess of \$1,000 per calendar year within the prior five (5) calendar years or (b) whether the persons or entities identified in (a) above have had any formal involvement within the prior five (5) calendar years with a community or not-for-profit organization with a central purpose of influencing public policy related to budgetary and fiscal policy which directly or indirectly relates to the continued availability and long-term viability of defined benefit pensions in the public sector, to education policy, or to retirement security policy.

REQUIRED DISCLOSURES

For the purposes of this disclosure, an organization has the “central purpose” of influencing policy if it is understood with the exercise of reasonable due diligence, including but not limited to the examination of the organization’s IRS filings and other publicly-available statements of purpose, that the organization intends to affect policy or engage in lobbying or other advocacy activity. A Respondent is not required to disclose contributions to organizations that engage in such activities in furtherance of providing medical research, aid to the poor, disaster relief, or other such tangible goods or service. The Trustees have determined that the following organizations presently fall under this required disclosure:

American Enterprise Institute,
American Legislative Exchange Council,
Brookings Institution,
California Common Sense,
California Policy Center,
Civic Committee of the Commercial Club,
Heritage Foundation,
Howard Jarvis Taxpayers Association,
Illinois Municipal League,
Illinois Policy Institute,
Independent Institute,
Jessie Ball DuPont Fund,
Laura and John Arnold Foundation,
Mackinac Center for Public Policy,
Manhattan Institute for Policy Research,
Massachusetts Taxpayers Foundation,
Mercatus Center at George Mason University,
National Council on Teacher Quality,
National Institute for Labor Relations Research,
Nelson Rockefeller Institute of Government,
National Taxpayers United of Illinois,

REQUIRED DISCLOSURES

Pioneer Institute,
R Street Institute,
Reason Foundation,
Show Me Institute,
State Policy Network,
StudentsFirst,
Taxpayers for Sustainable Pensions,
Taxpayers United of America,
Teacherspensions.org,
Texas Public Policy Foundation,
The Future of Freedom of Foundation,
The Pew Charitable Trust,
UnionWatch,
Urban Institute,
Wyoming Liberty Group, and
Any state or local affiliates or chapters of the above organizations.

[Sentinel Response: None.](#)

(iv) The Respondent and any parent, controlling entity, subsidiary, or affiliate must disclose any direct or indirect financial relationships, transactions, or consulting agreements with the Chicago Board of Education entered into within the prior five (5) calendar years. Any such direct or indirect financial relationships, transactions, consulting agreements, or consulting-related contracts with the Chicago Board of Education entered into on or after the execution of an agreement shall be identified in an amended Respondent Disclosure within thirty (30) calendar days of any new relationship, transaction, investment, agreement, or contract with the Chicago Board of Education.

[Sentinel Response: None.](#)

(v) The Respondent must disclose the names and addresses of any subcontractors and the expected amount and/or percentage of money each will receive under the agreement if authorized by the Fund.

[Sentinel Response: None.](#)

REQUIRED DISCLOSURES

(vi) The total number of Respondent’s staff. The number of Respondent’s staff and percentage of its staff, broken out separately for each category, who are (1) a minority person, (2) a female, or (3) a person with a disability. This information must be provided using the EEOC chart available on CTPF’s website. Supplemental information to the EEOC chart is welcome.

Sentinel Response:

JOB CATEGORIES	HISPANIC OR LATINO		NOT-HISPANIC OR LATINO											OVERALL TOTALS		
	*****MALE*****											*****FEMALE*****				
	MALE	FEMALE	WHITE	BLACK OR AFRICAN AMERICAN	NATIVE HAWAIIAN OR PACIFIC ISLANDER	ASIAN	AMERICAN INDIAN OR ALASKAN NATIVE	TWO OR MORE RACES	WHITE	BLACK OR AFRICAN AMERICAN	NATIVE HAWAIIAN OR PACIFIC ISLANDER	ASIAN	AMERICAN INDIAN OR ALASKAN NATIVE		TWO OR MORE RACES	
EXECUTIVE/SR OFFICIALS & MGRS	1	1	20	0	0	0	0	0	4	0	0	0	0	0	26	
FIRST/MID OFFICIALS & MGRS	0	0	23	2	0	2	0	0	8	0	0	1	1	0	37	
PROFESSIONALS	25	5	251	20	0	30	3	7	38	5	0	9	0	3	396	
TECHNICIANS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
SALES WORKERS	4	0	79	2	1	0	0	0	11	0	0	0	0	0	97	
ADMINISTRATIVE SUPPORT	2	2	10	1	0	0	0	0	25	4	0	1	0	3	48	
CRAFT WORKERS	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	
OPERATIVES	0	0	1	1	0	0	0	0	0	0	0	0	0	0	2	
LABORERS & HELPERS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
SERVICE WORKERS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
TOTAL	32	8	385	26	1	32	3	7	86	9	0	11	1	6	607	
PREVIOUS REPORT TOTAL	31	4	347	22	1	26	2	4	63	14	1	6	0	5	526	

(vii) The number of current contracts that the Respondent has with a (1) minority owned business, (2) female owned business, or (3) business owned by a person with a disability.

Sentinel Response: Sentinel has vendor contracts in place with six (6) MBE’s, four (4) WBE’s and two (2) Veteran entities.

(viii) The number of current contracts that the Respondent has with a business other than (1) a minority owned business, (2) a female owned business, or (3) a business owned by a person with a disability, under which, while the business is not owned by one of the above categories, where more than fifty percent (50%) of services performed pursuant to the contract are performed by (1) a minority person, (2) a female, or (3) a person with a disability.

Sentinel Response: None.

(ix) The Respondent shall agree to annually disclose various EEO data and diversity of vendor’s contracts as required by the Fund.

Sentinel Response: Sentinel will comply.

K. Exhibits and Attachments

a. Any additional information or exhibits appropriate for CTPF's consideration may be included under this category.

[Sentinel Response: Please see below Exhibits.](#)

Exhibit I: Sample – Managed Services Scope of Work

EXECUTIVE SUMMARY

Sentinel Technologies, Inc. (Sentinel) is honored to be able to provide a NOC Monitoring and Managed Services solution for Chicago Teachers Pension Fund.

For more than 40 years, Sentinel has been recognized as a top-tier business technology solutions and services provider dedicated to delivering the highest quality Customer service and support. Even as our services have spanned generations of technology, Sentinel has stayed at the forefront of IT developments and maintained a singular focus on providing practical and innovative solutions. With single-source accountability, Sentinel's proven repeatable methodology, processes and experienced teams can efficiently address a full range of IT needs - from NOC monitoring and managed services, to communications, to data center, to cloud solutions, to business process improvement and assessments, to targeted applications and end-to-end IT solutions. Our proven success has allowed us to expand from our original charter of providing technology maintenance services to our current standing as one of the leading IT services and solutions providers in the U.S. and beyond. Sentinel's engineers, Customer Service and support, and project management team's reputation has become synonymous with high quality, cost effective solutions for our customers. Sentinel's pricing response will reflect our sincere desire to establish a long-term partnership. Sentinel is confident we will emerge as the top option for executing your business critical managed services, but also as your preferred partner for contributing to your overall growth and future success.

Sentinel provides our customers with the complete solution: vision, design, product, implementation, documentation, service and support. Sentinel's services span the range of business verticals in the mid-market, upper mid-market, and enterprise level organizations. Companies in Financial and Banking, Healthcare, Government, Education, Legal, Utilities, and Manufacturing verticals have all taken advantage of Sentinel's ability to take either full responsibility or act as a supplemental contributor to our customer's most important business technology initiatives.

Headquartered in Downers Grove, IL, Sentinel Technologies has independently managed offices in nine locations: Chicago, IL, Springfield, IL, Milwaukee, WI, Phoenix, AZ, Detroit, MI, Grand Rapids, MI, Lansing, MI, Fort Lauderdale, FL and Denver, CO, allowing us to service our customers both nationally and internationally. Sentinel applies an extraordinary breadth of technical solution expertise to design, sell, deploy and support our customer's business technology needs. Our unwavering commitment to thought leadership and customer satisfaction maximizes both the value of technology investments and its impact to the business. When it comes to achieving a tangible ROI and sustainable performance from your IT environment, Sentinel stands apart. Sentinel's large service staff (650+ employees), multitude of original equipment manufacturers (OEM) certifications, a 24x7 Customer Care Center and a professionalism and commitment to service excellence act in combination to ensure a successful partnership.



SENTINEL MONITORING SYSTEM & SUPPORT OVERVIEW

The diverse nature of today’s Local and Wide Area Networks creates support challenges for many organizations. Sentinel Technologies’ Monitoring and Managed Service offerings address these challenges by providing specialized resources to support customers’ systems.

Sentinel has been delivering mission critical network support services to customers since 1982. Our goal is to provide our customers with peace of mind knowing their network is being monitored by professionals 24 hours/day, 7 days/week. Through years of experience in working with Network Operations Centers (NOC), Sentinel has developed a unique and well rounded perspective on how to provide value through monitoring services. It is not just dials, graphs and trend lines – the real value lies in avoiding outages and minimizing the impact if an outage occurs.

NOC Monitoring and Managed Services Benefits:

- **Reduce Downtime** by ensuring systems are monitored and remediation is delivered 24x7x365 with industry leading SLAs.
- **Stabilize Costs** by creating a predictable cost model offering predefined, all-inclusive management and administration cost per device.
- **Improved business continuity** with SLA bound infrastructure availability and performance through 24x7x365 proactive monitoring and support via Sentinel’s dedicated Network Operations Center.
- **Reduced risk of employee turnover** creating uncertainty and inconsistency in the operations. Sentinel’s Managed Services will provide a level of continuity and consistency.
- **Increase IT support coverage** through utilizing Sentinel’s dedicated 24x7x365 Network Operations Team who specializes in day-to-day operations and maintenance.
- **Provide single number resolution** to IT infrastructure services delivery.
- **Deliver infrastructure services elasticity** providing fixed rate supplemental IT services.
- **Enhanced Infrastructure Reliability** by leveraging the breadth of experience available through Sentinel’s extensive technical staff to support a wide range of technologies.



STABILIZE COSTS



INCREASE SYSTEM HEALTH



STAY FOCUSED

SCOPE OF WORK

Sentinel NOC Remote Monitoring and Managed Services

Sentinel offers full managed services and monitoring solutions for advanced visibility into performance and utilization of resources at great scale. Based on multiple proven platforms, advanced correlation services and multiple alerting options, Sentinel has built an industry leading Network Operations Center (NOC).

Sentinel NOC Remote Monitoring features include:

- NOC 24 x 7 Remote Monitoring via a secure VPN tunnel.
- Up/Down status monitoring via ICMP requests.
- Availability / Uptime.
- Syslog/Trap storage.
- Hardware Device Monitoring and Analysis.
- CPU, Memory, Disk space and Latency.
- WAN Circuit status.
- Traffic throughput, utilization, errors and discards of WAN circuits, Trunk ports or any critical interface.
- Wireless Monitoring – AP association status, SSID, Signal Strength, Wireless clients.
- Alerting (built with intelligence that eliminates false positives).
- Alert Routing to NOC and/or dedicated engineer for immediate remote resolution.
- Hardware Health Reporting (fan, power supplies, temperature, environmental, and the like).
- Reporting (Inventory, Utilization, Performance, and much more).
- PRI circuits – monitors the status and capacity of your PRIs.
- Voice Gateways - monitors the status and utilization of your voice gateways.

Managed Services Feature Highlights

- **Sentinel Remote Diagnosis and Remote Repair Capability.**

Sentinel leverages remote tools to ensure 24x7x365 support service is delivered quickly and efficiently. Sentinel understands that your IT environment is dynamic and demands visibility and expert engineers around the clock and will stay committed to providing continuous effort and support.

- **Carrier Incident Handling.**

Sentinel will work with carriers on resolving circuit issues and outages. Sentinel has numerous levels of escalation points through multiple carriers due to the maturity and multiple years of experience providing carrier incident handling.

- **Configuration Management.**

Sentinel will automatically back up system configurations on network devices and any device that has a CLI (Command Line Interface). Configurations are backed up nightly and stored in an encrypted database *only* if a change has occurred.

Sentinel will automatically back up system configurations on the following devices. Configurations, Change Reports and on-demand download ability are available in the NOC web console. The following methods will be used to back up the environment:

Device Type	System Config Backups
Routers	NOC via CLI
Switches	NOC via CLI
Firewalls	NOC via CLI
Wireless Controller	NOC via CLI
Storage Array	TBD

- **Sentinel Complete Restore.**

In the event of hardware failure, hardware replacement, catastrophic outage causing corrupt config, or any loss of system configuration, Sentinel maintains backed up configurations so systems can be restored promptly, providing minimal downtime in the event of an outage (*restoration only applies to backed up equipment listed above*).

- **Sentinel End-To-End Problem Management.**

Sentinel will provide management and support services on any equipment covered under the agreement. It is understood that at times, manufacturers or third party providers might need to be engaged for further support. Sentinel will work with agents in attempting to resolve issues as long as maintenance and a LOA (letter of agency) is maintained.

- **Device Administration.**

Sentinel will provide dedicated expert engineers to administer covered systems on a 24x7x365 basis. Unlimited Moves, Adds and Changes are included to assist with your day to day administration. A best practice guideline of 2 hours will be used on change tickets.

- **Preventative Maintenance and Patching.**

Manufacturer releases are important for staying up to date with critical software and security patches. Sentinel will work with on a strategy for this preventative maintenance while taking into account your change control guidelines and approval process. A detailed report of system updates will be provided during the following intervals with recommendations and Scope of Work.

Firmware updates and minor release updates are included in the following schedule.

Device Type	Level	Review Frequency	Performed
Routers	Minor	6 Months	As Needed or Requested
Switches	Minor	6 Months	As Needed or Requested
Firewalls	Minor	3 Months	As Needed or Requested
Wireless Controller	Minor	6 Months	As Needed or Requested
Storage Array	Minor	6 Months	As Needed or Requested
Windows Servers	Minor	Monthly	Automated

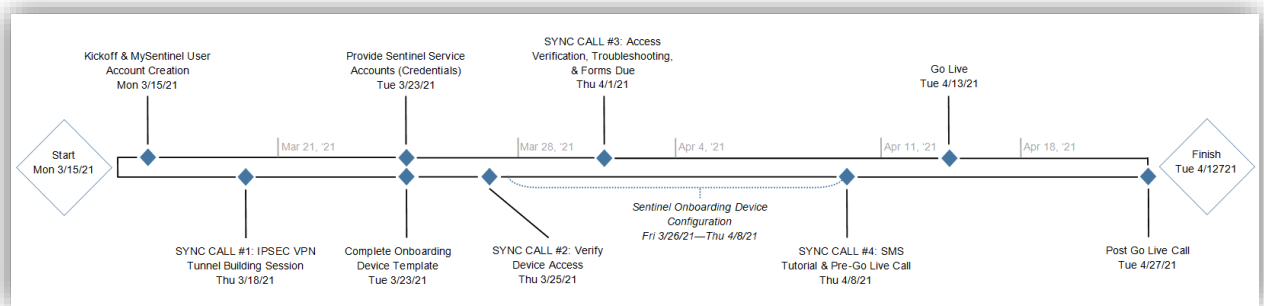
- **Immediate Leverage of ACTS (formerly HANS™) Maintenance Contracts.**

With NOC Monitoring in place, Sentinel will be able to provide a prompt and efficient response and remediation when ACTS™ or SMARTnet maintenance contracts are in place.

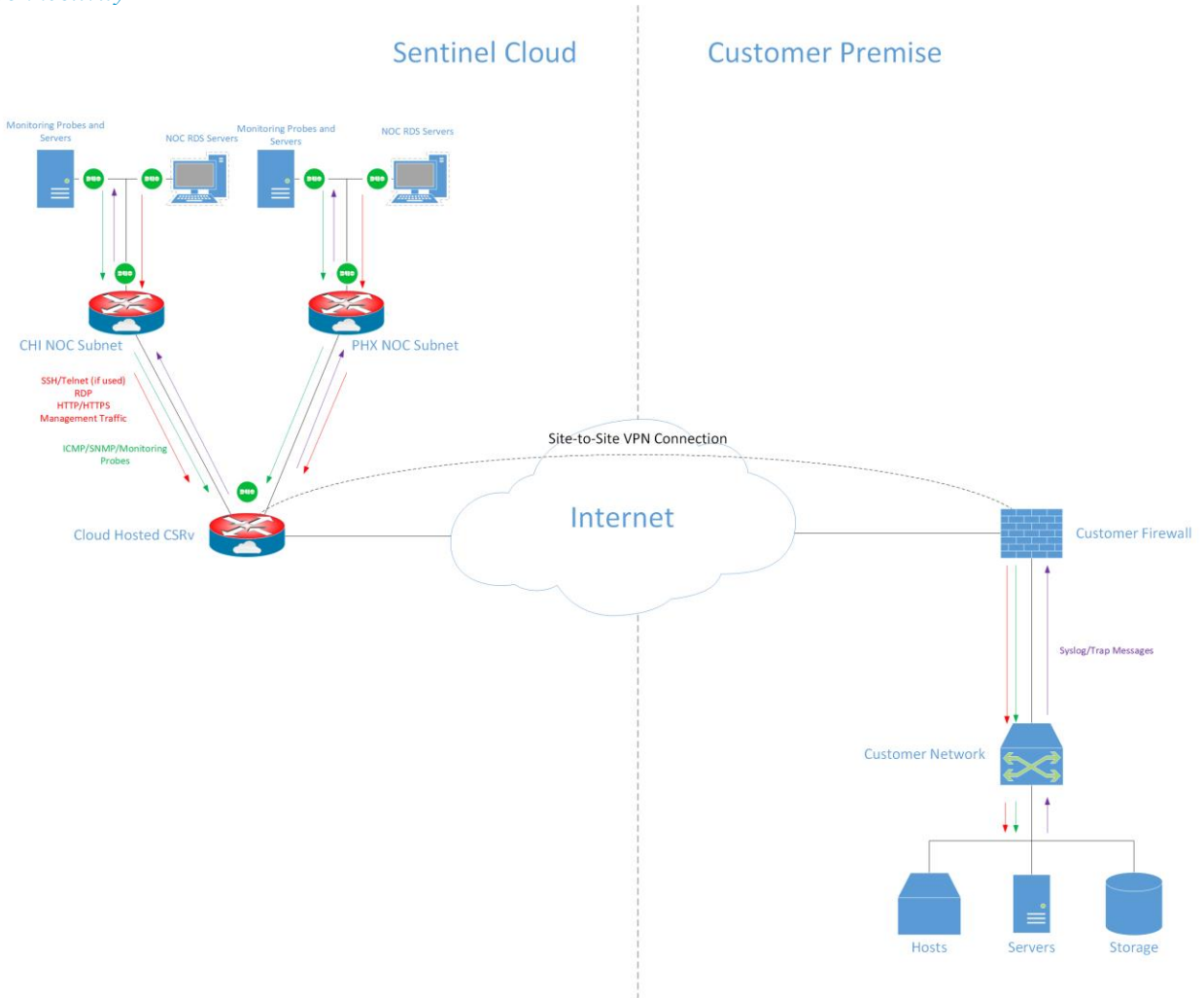
NOC Onboarding

Sentinel utilizes PMI best practices for the onboarding of Managed Services Customers. During the onboarding and transition period of the managed services engagement, Sentinel will define key stakeholders necessary to execute all onboarding responsibilities (e.g. PMs SDMs, SMEs, etc.), and document any risks that could affect the onboarding project.

To ensure complete transition within 30-45 days, Sentinel will provide a complete project plan and work breakdown structure outlining the tasks and responsibilities of the onboarding phase. Sentinel will execute all necessary tasks outlined within the work breakdown structure in order to complete the project on time, and as needed we will assist with gathering any information required to complete the Customer Onboarding Forms. Once all the required onboarding forms are complete and credentials have been created to allow Sentinel access to the network, the Sentinel onboarding Project Manager will engage engineering resources to configure and establish VPN connectivity to the NOC network. After connectivity has been established to the network and access has been granted to all applicable devices, the Sentinel onboarding engineer will execute or assist with all necessary configurations to establish connectivity to each device. Following the completion of all devices being monitored, the Sentinel onboarding team will conduct training on how to navigate and utilize the features within our Sentinel Monitoring System. The onboarding team will cross train and hand over all findings that have been discovered during the onboarding phase to the dedicated support teams. Once the project plan has been fully executed and all work has been accepted, you will be officially transitioned to the NOC and managed services team that will be supporting the core technologies: network, server, and security.

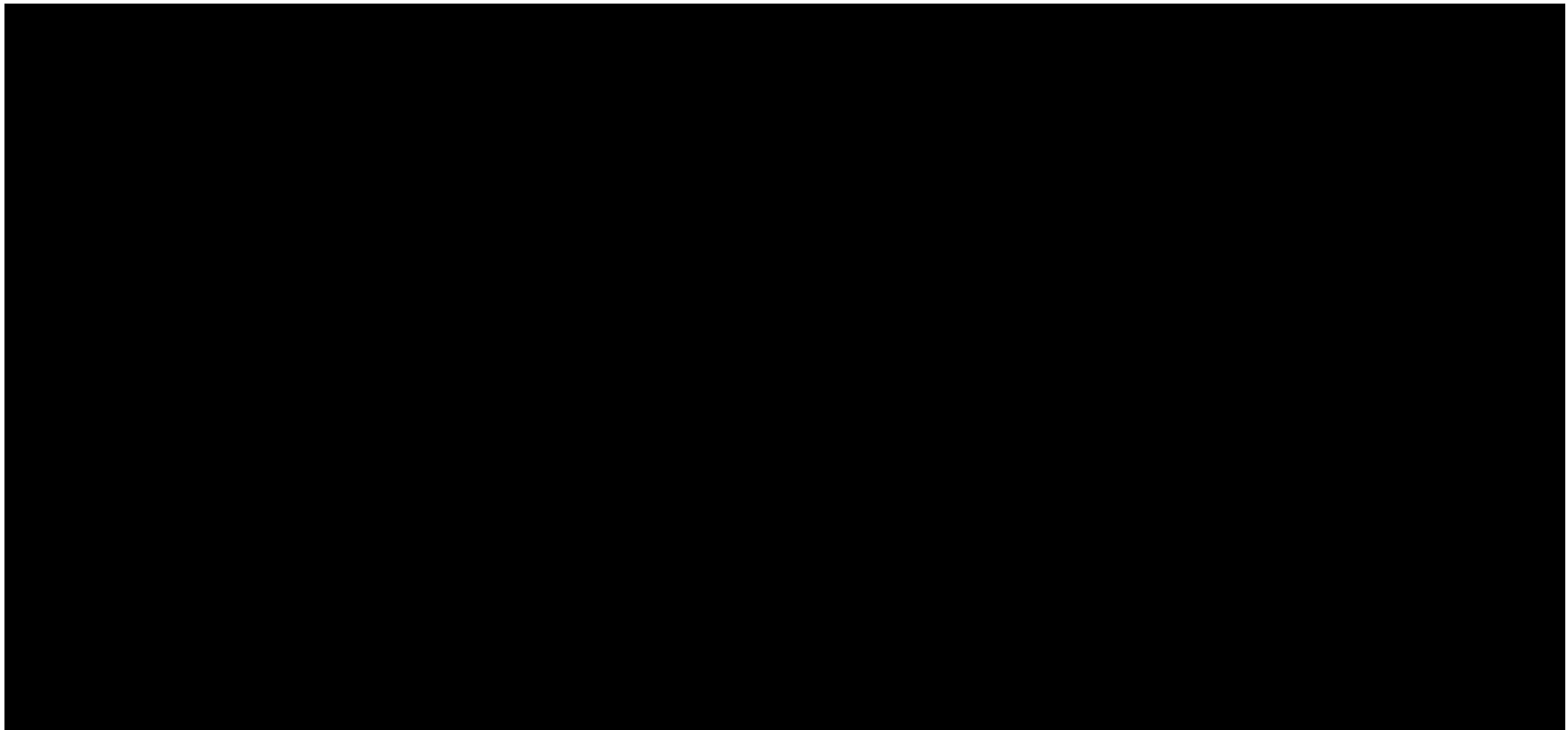


Connectivity

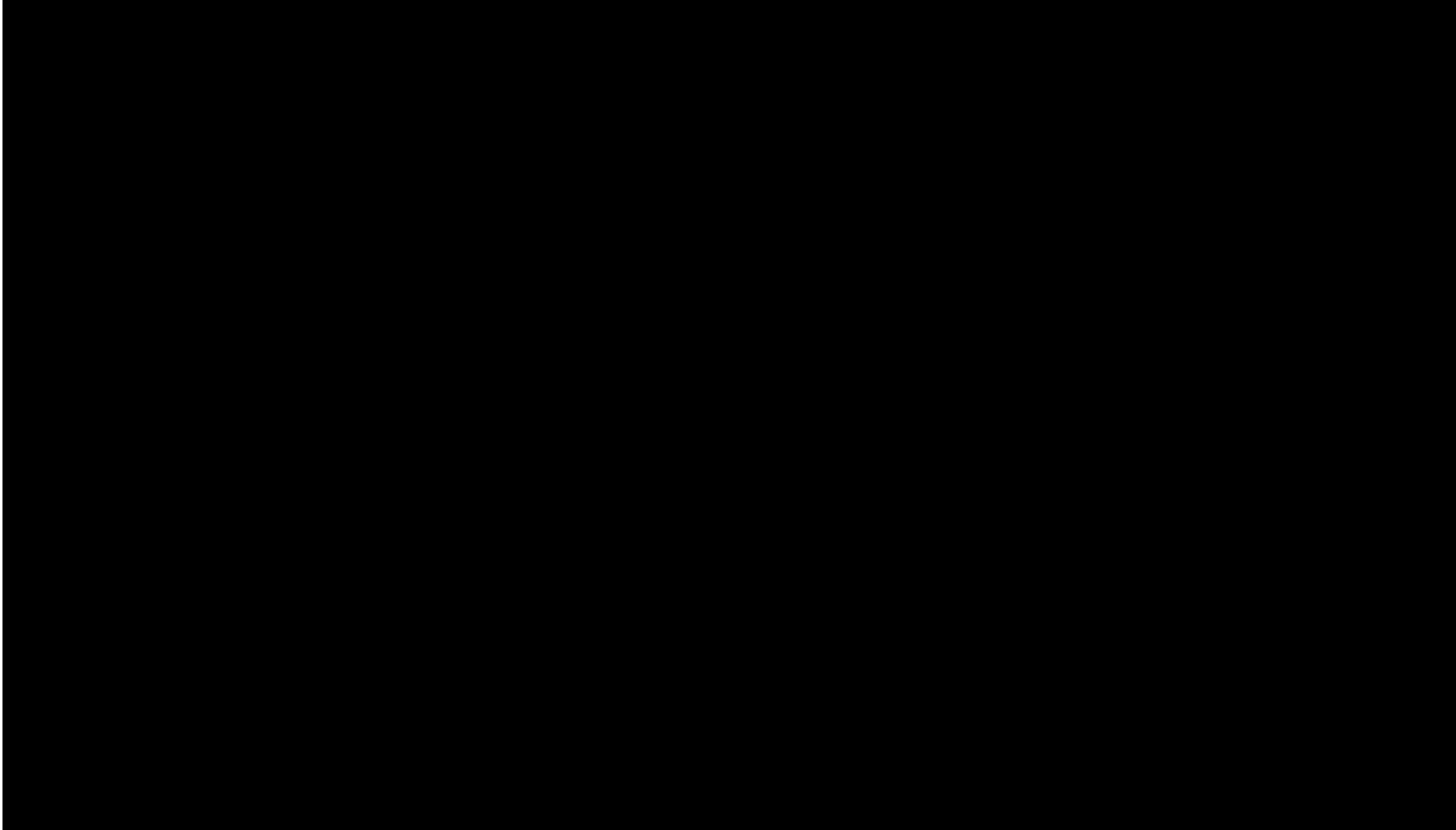


QUALITY ASSURANCE

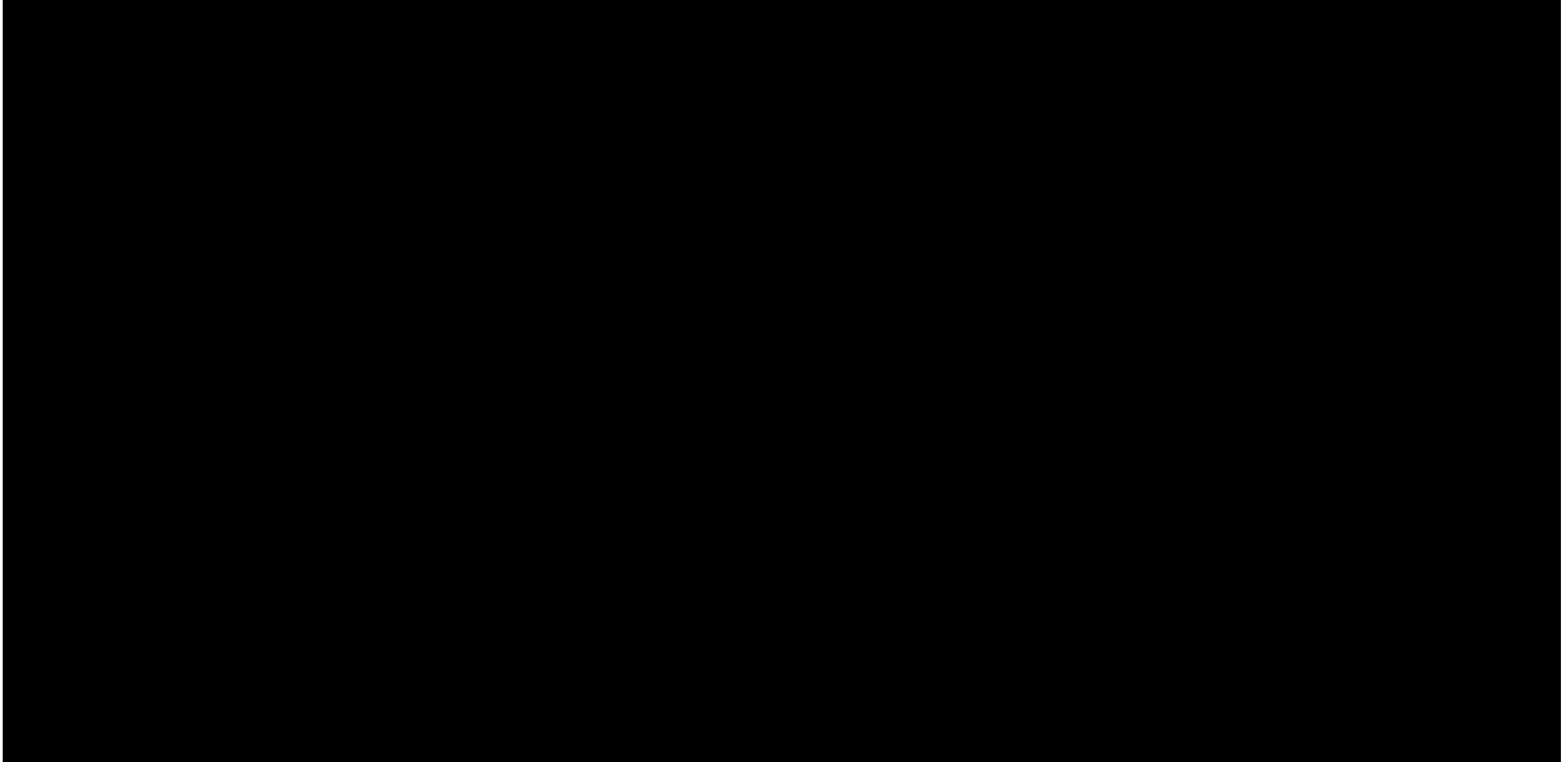
Sentinel's Quality Assurance team will host regularly scheduled review meetings to review NOC monitored data, uptime & availability, traffic patterns, root cause analyses of chronic issues, trouble ticket data and SLAs, and help identify environment trends or capacity issues. Additional dashboards within ServiceNow will show an executive view into the performance, availability, usage and equipment inventory. Below are sample dashboards:



EXHIBITS AND ATTACHMENTS

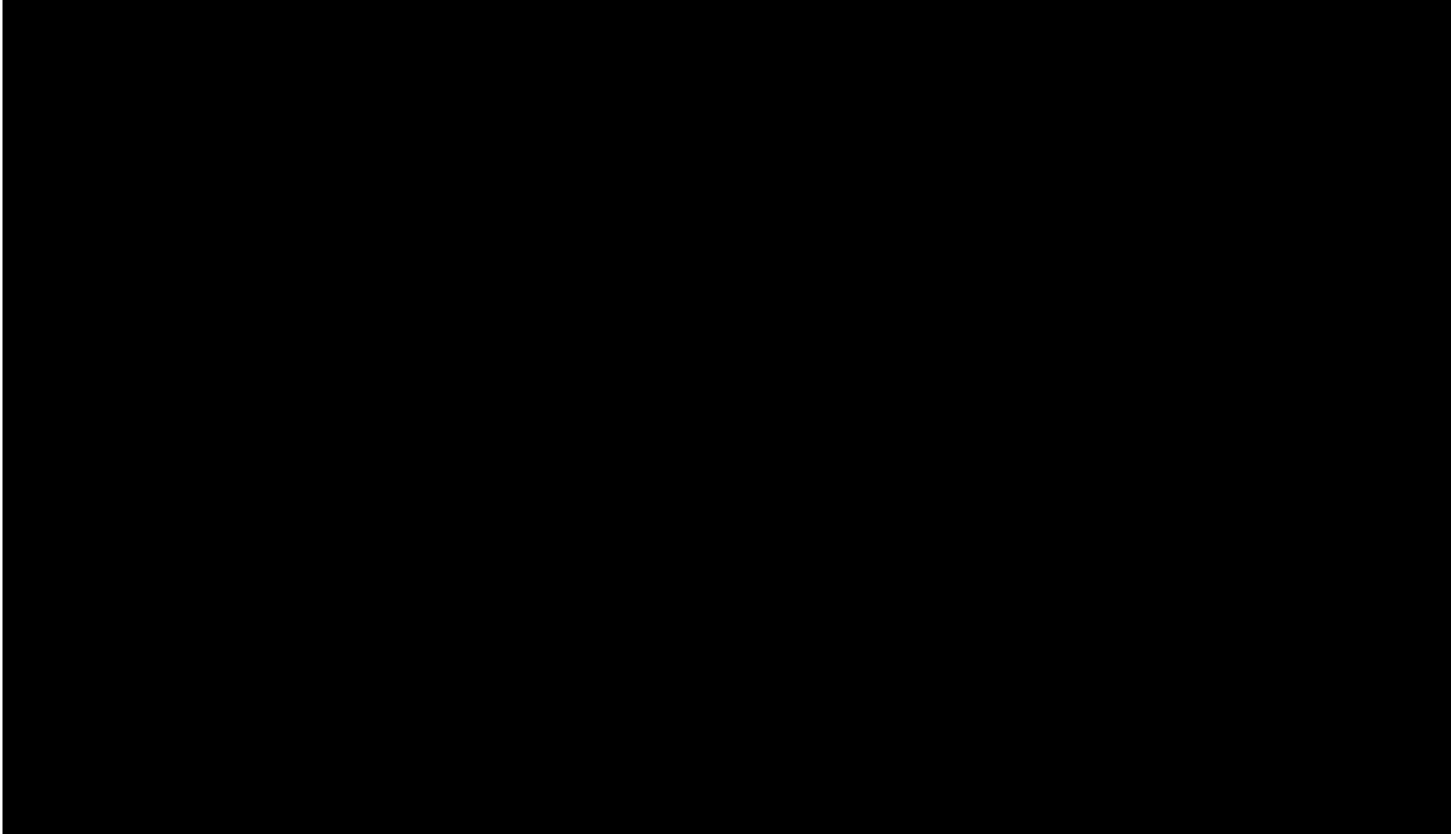


EXHIBITS AND ATTACHMENTS



PORTAL ACCESS & VIEWS

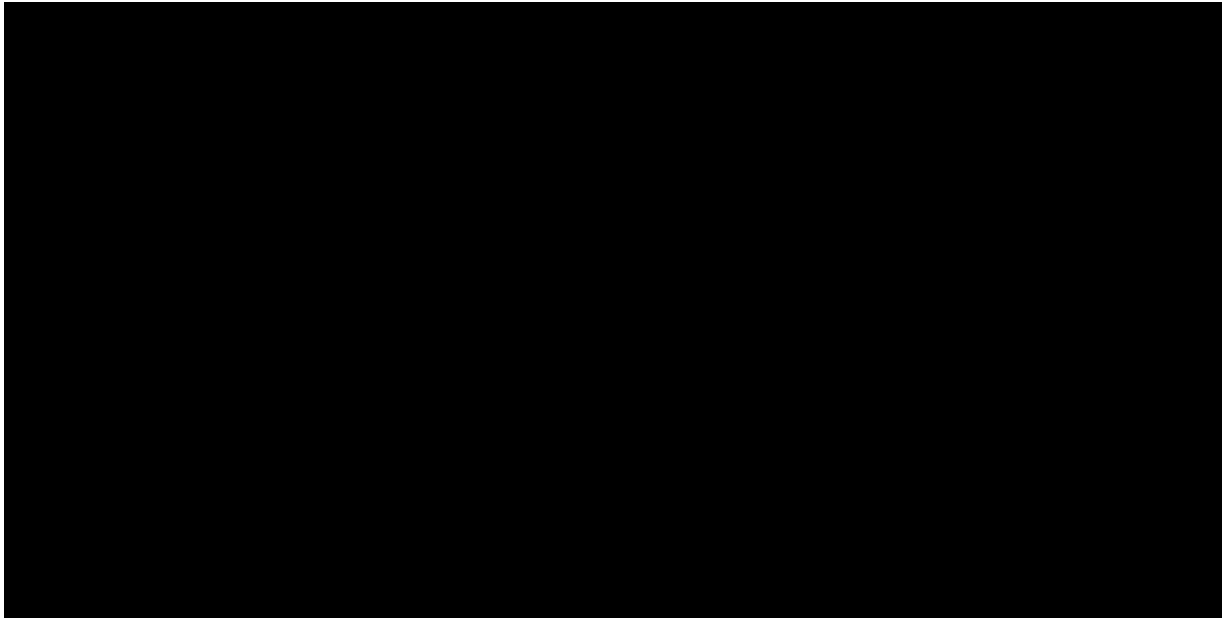
Main Portal



SERVICE LEVEL AGREEMENTS

Sentinel makes commitments to industry leading SLAs within NOC Monitoring & Managed Services. SLAs are defined from first communication to a MTTR (Mean Time to Repair) for incidents and change tickets. All SLAs are tracked and worked through Sentinel’s trouble ticketing system, ServiceNow, and reporting is made available through the ticketing console on www.sentinel.com.

The following is a matrix of Sentinel’s SLAs built on industry standards (ITIL) Urgency/Impact definitions.



Sentinel guarantees the following SLAs and will report on SLA performance through automated reporting and the monthly quality assurance review meetings.

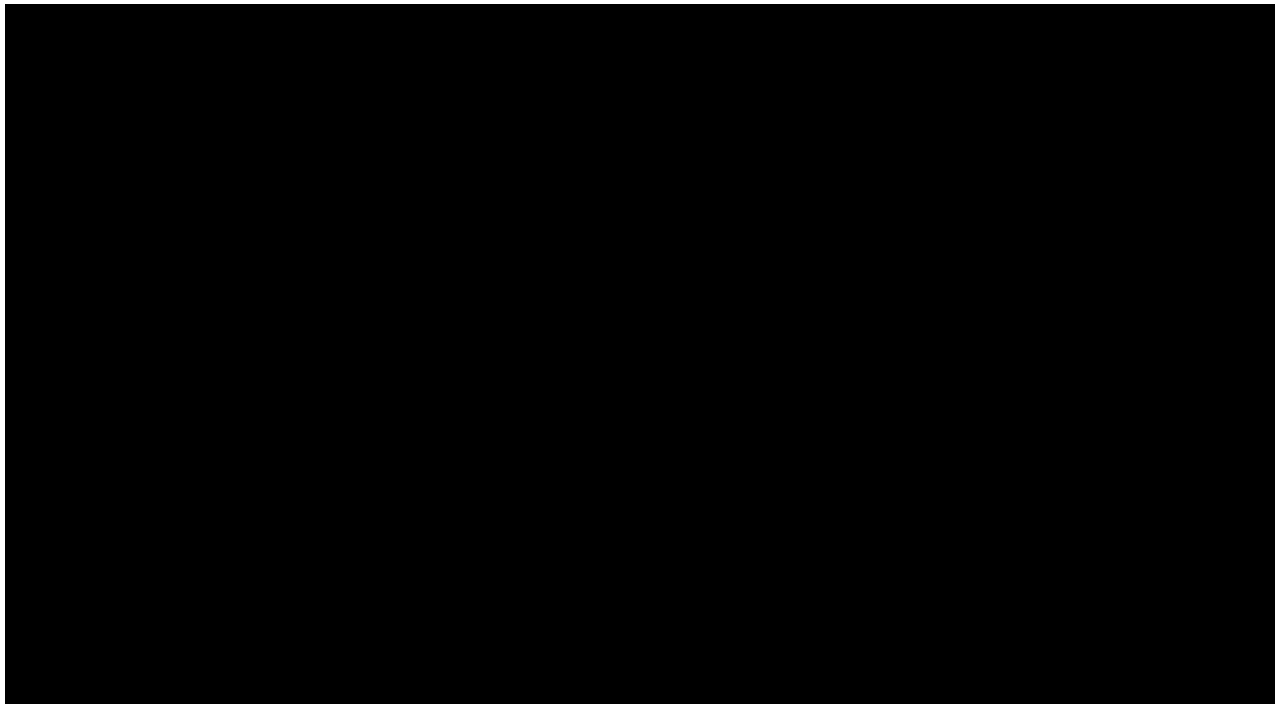
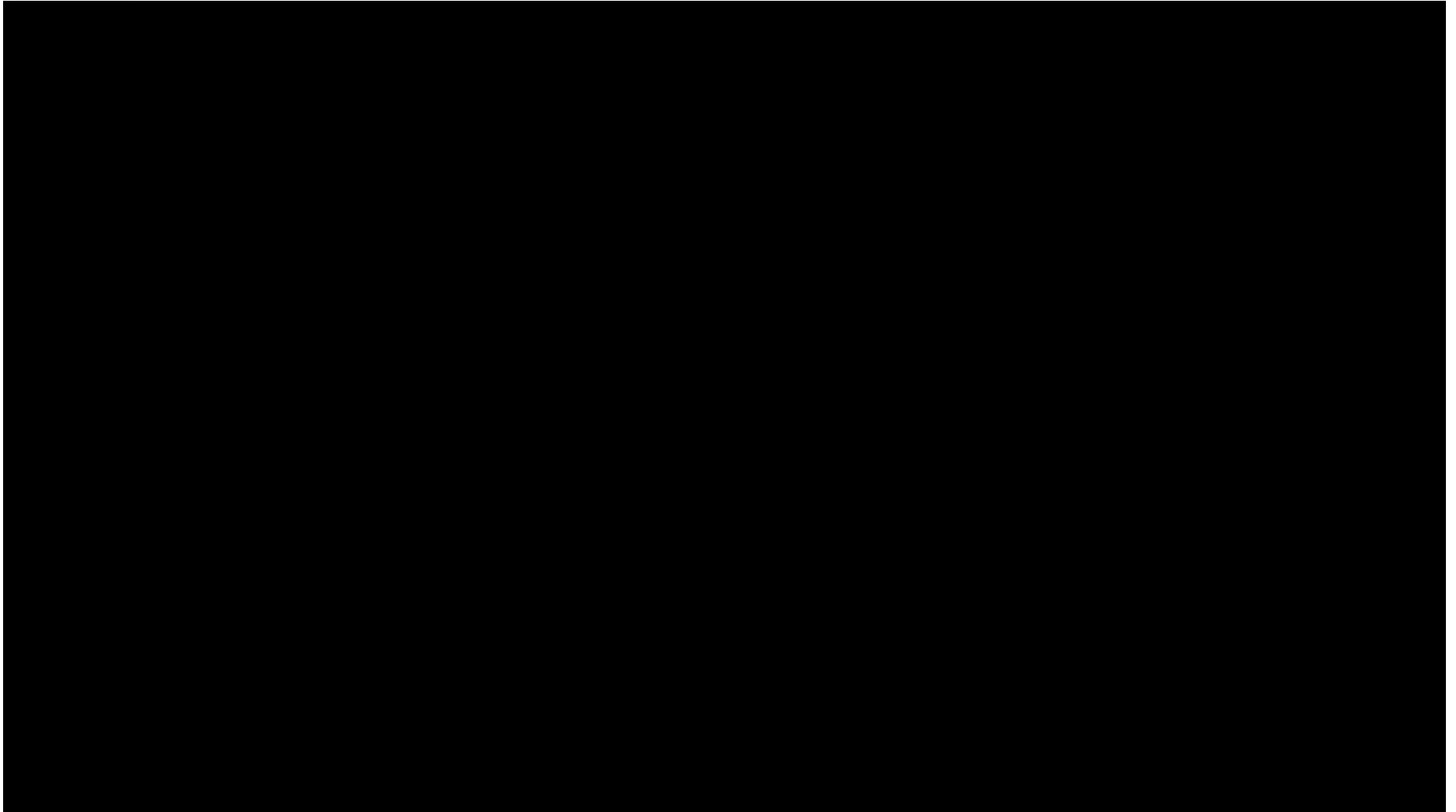
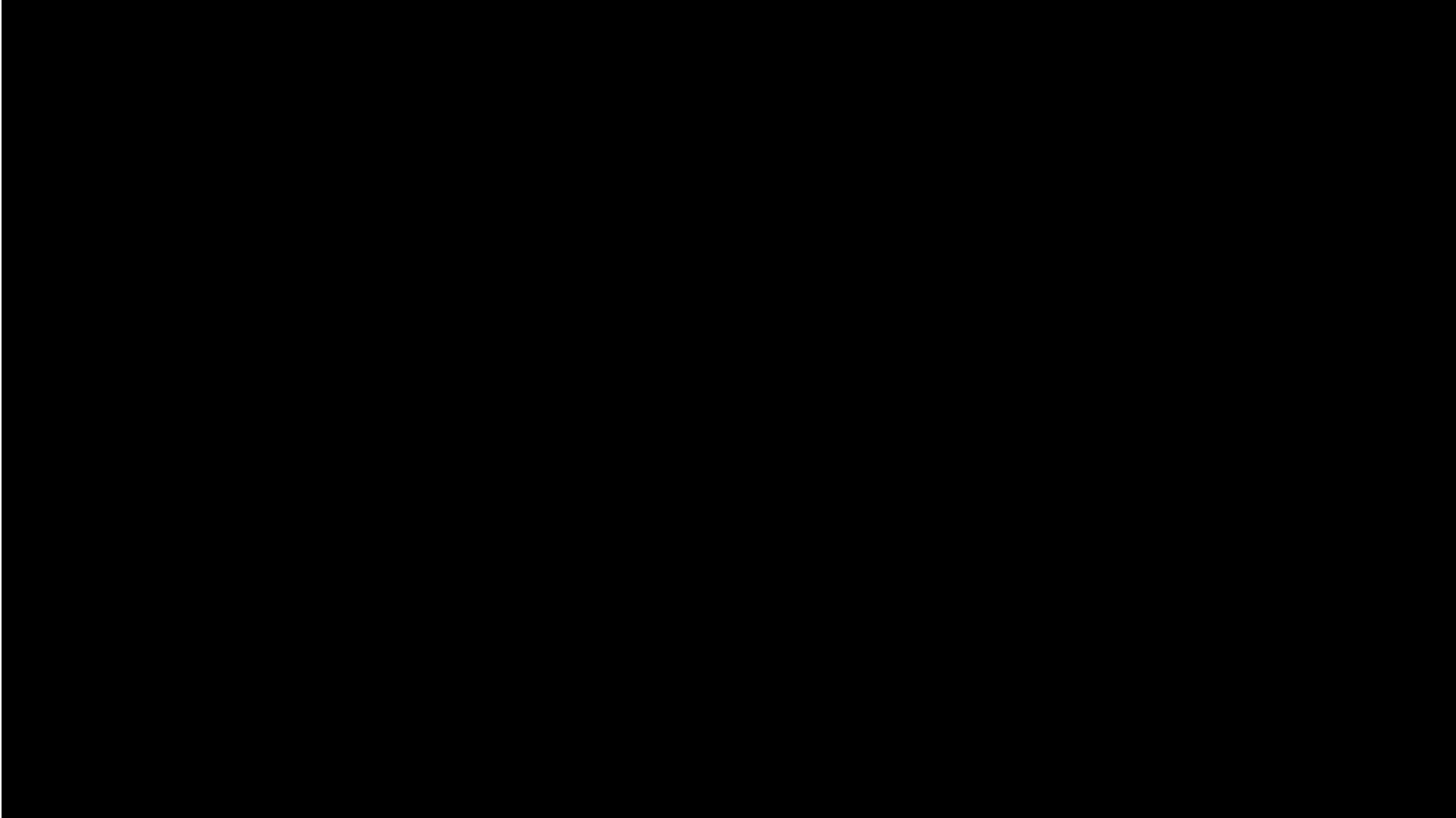


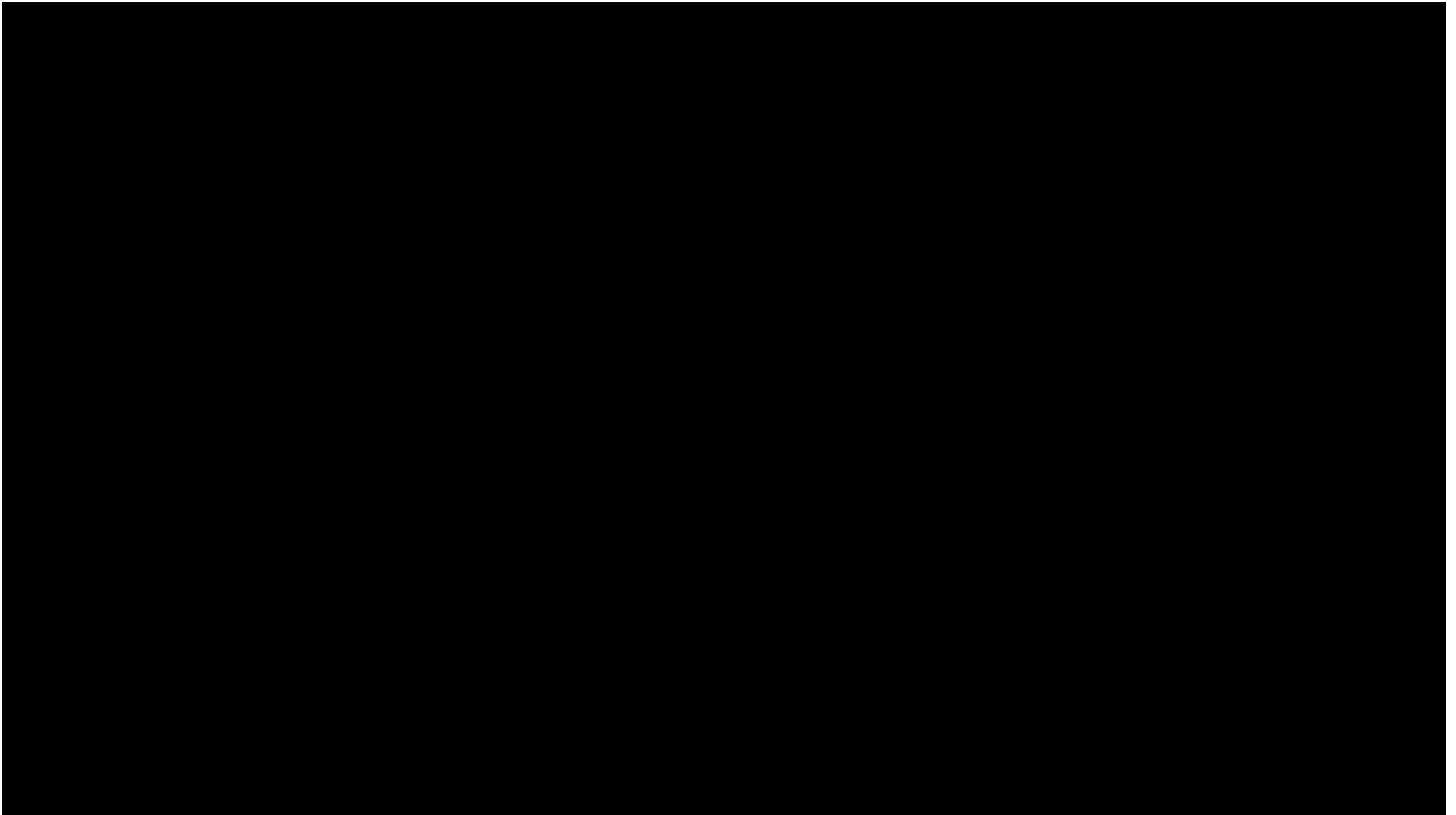
Exhibit II: Additional Deliverables or Services



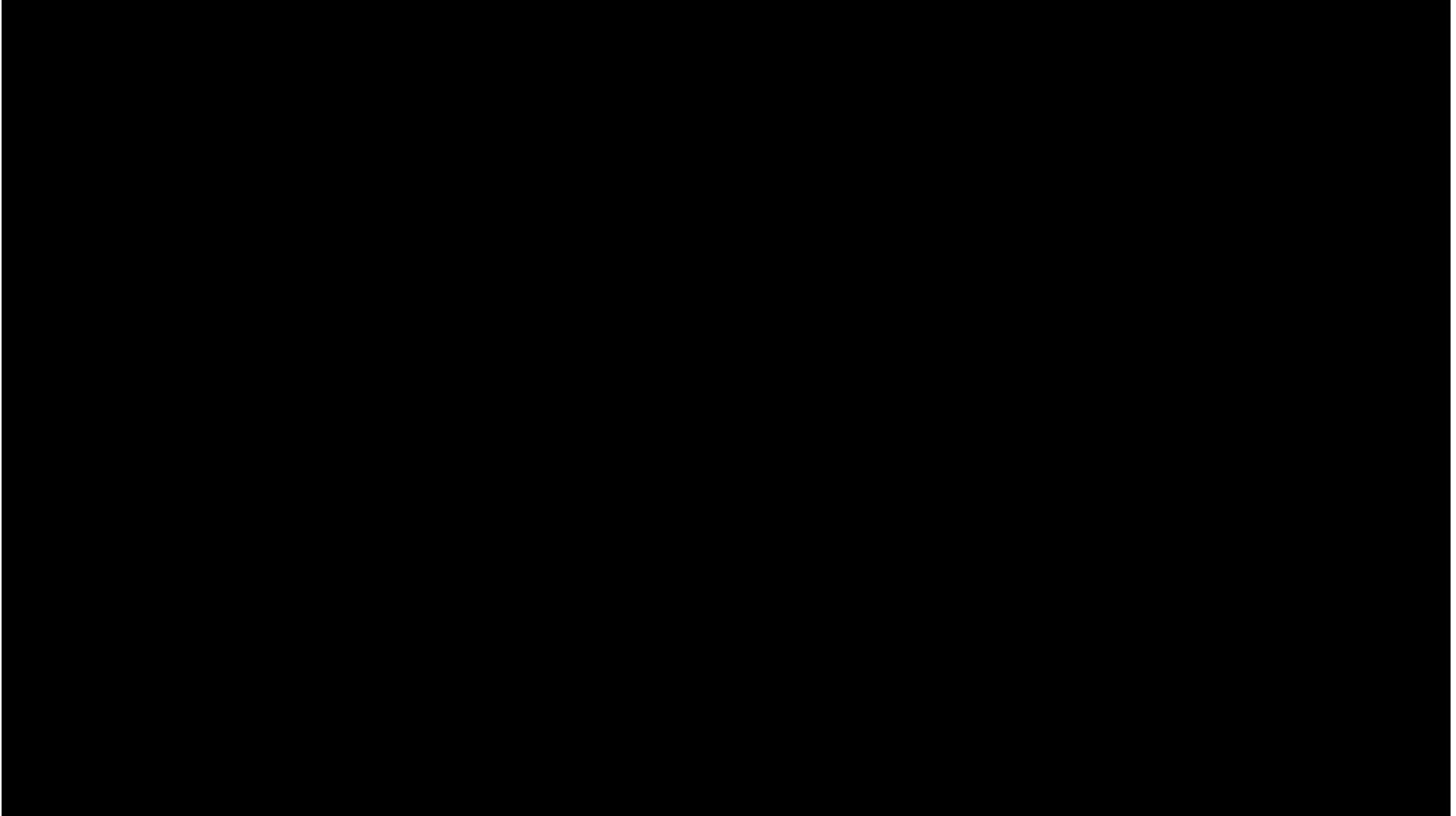
EXHIBITS AND ATTACHMENTS



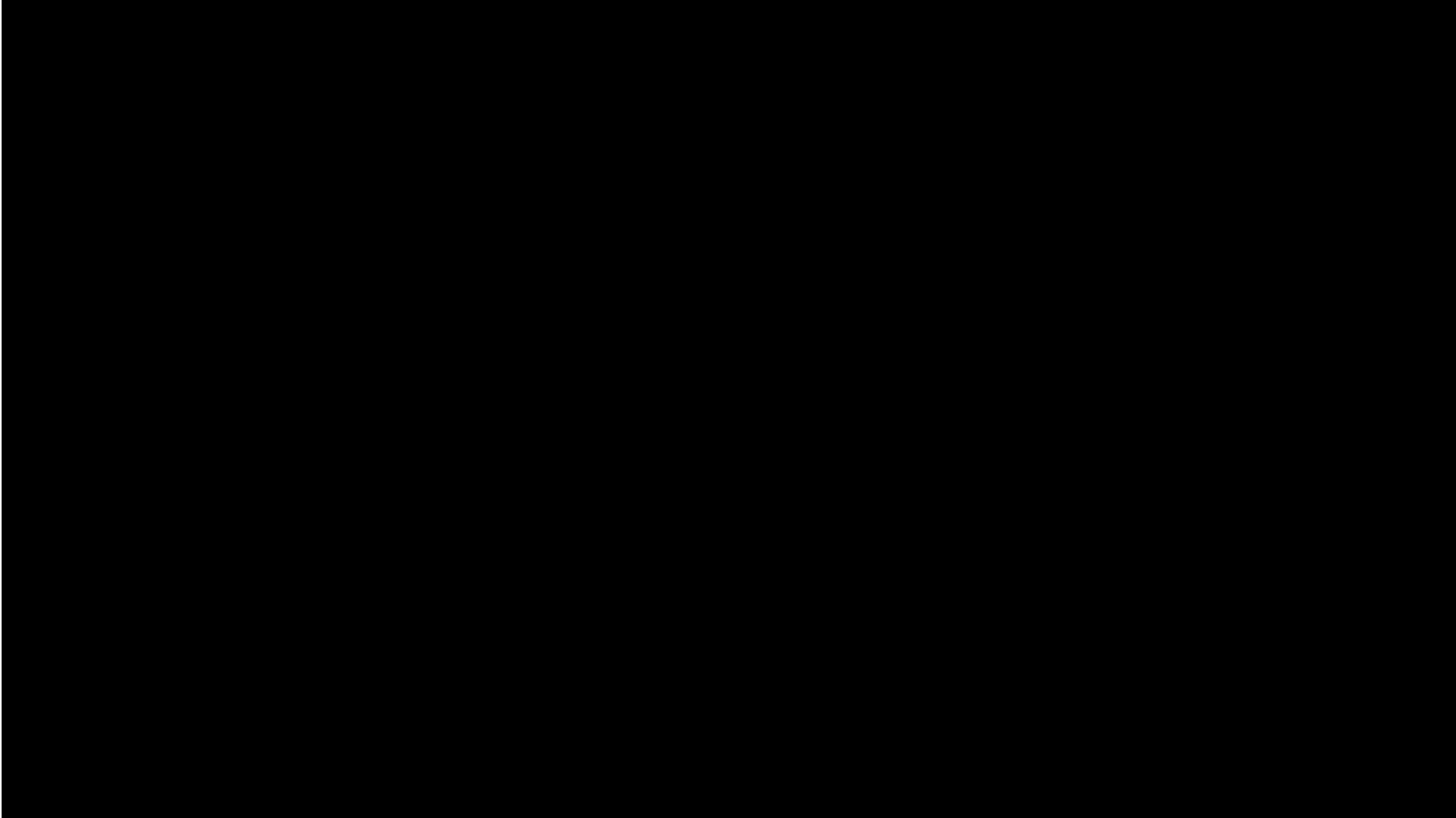
EXHIBITS AND ATTACHMENTS



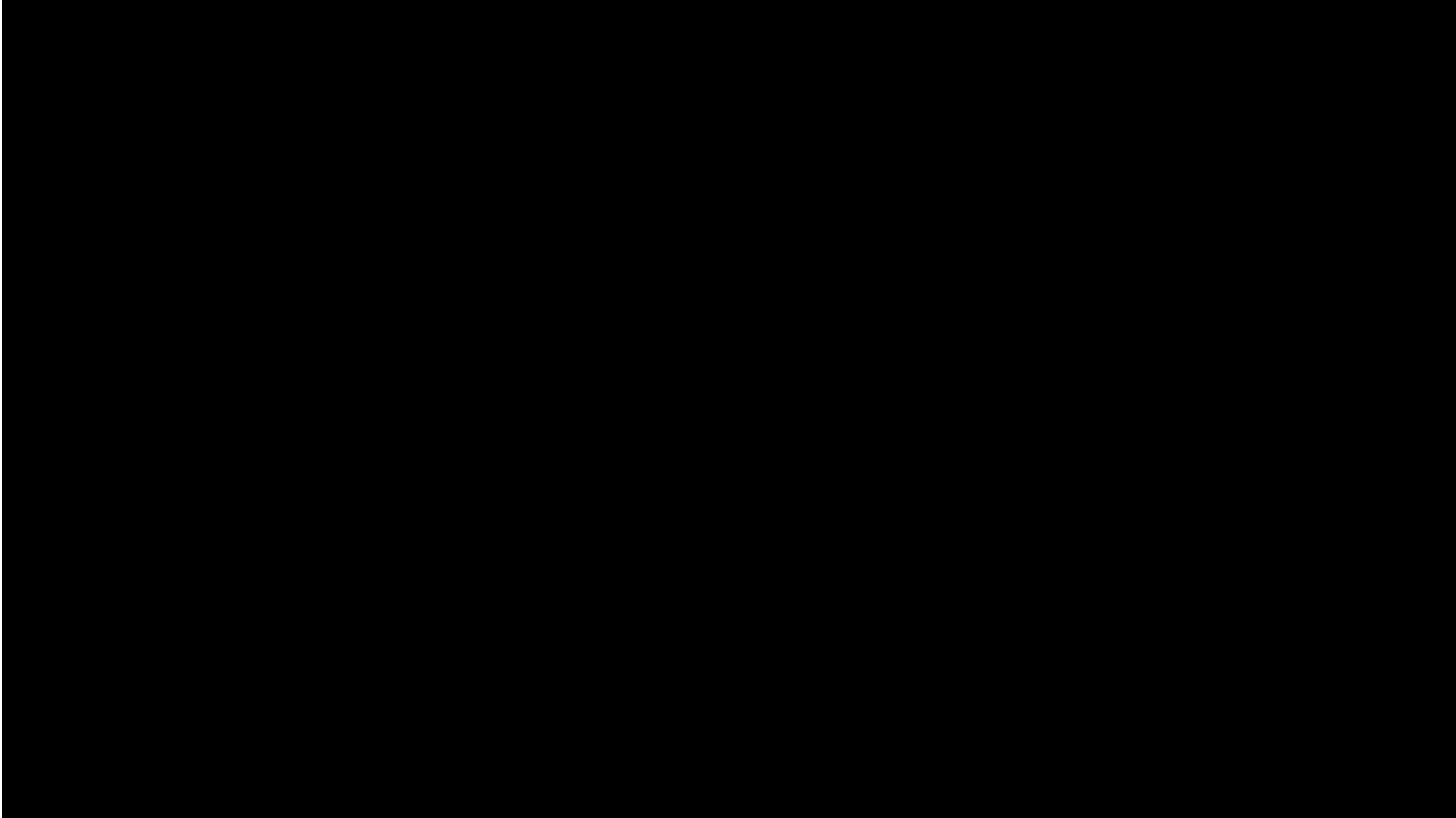
EXHIBITS AND ATTACHMENTS



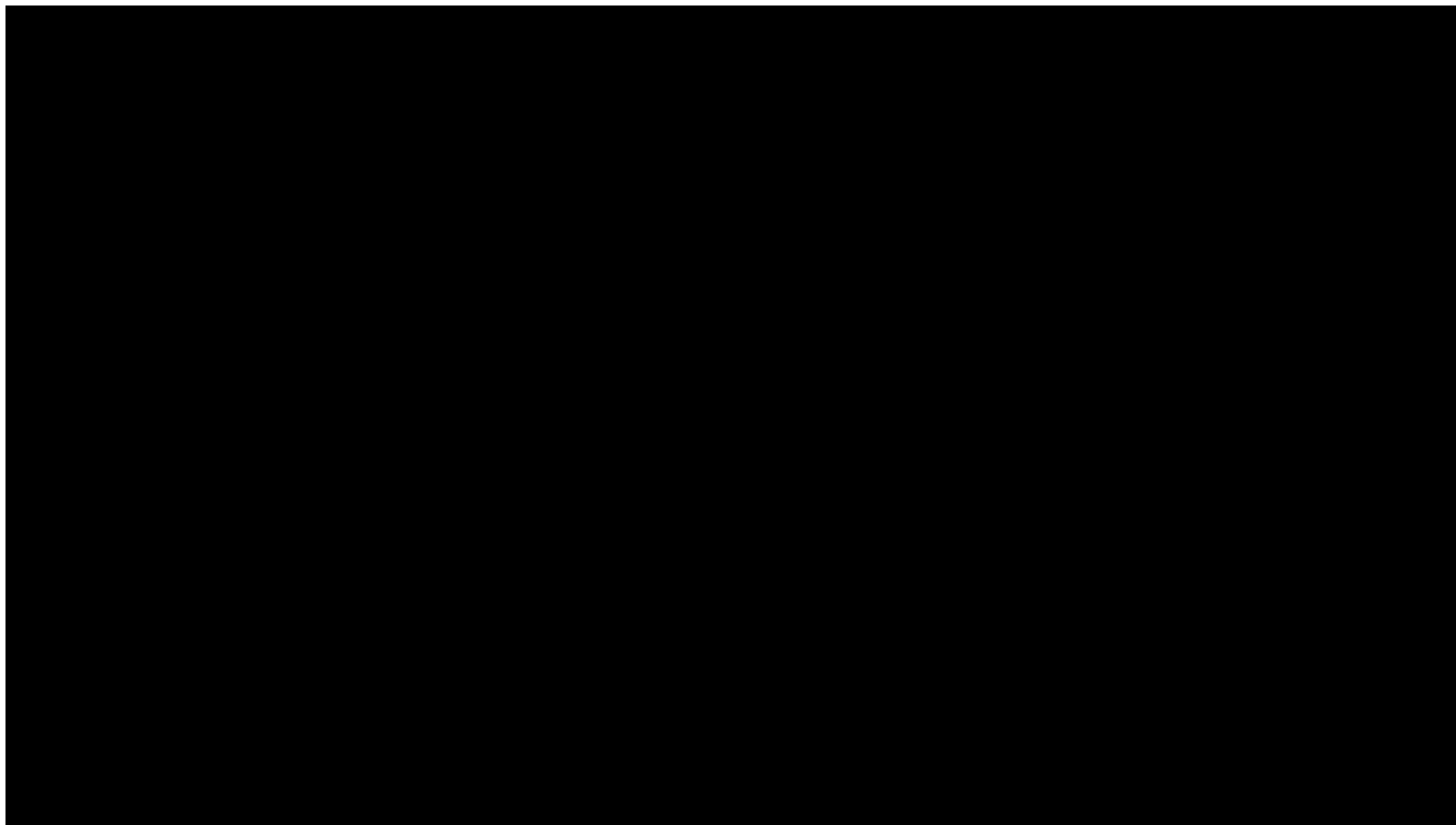
EXHIBITS AND ATTACHMENTS



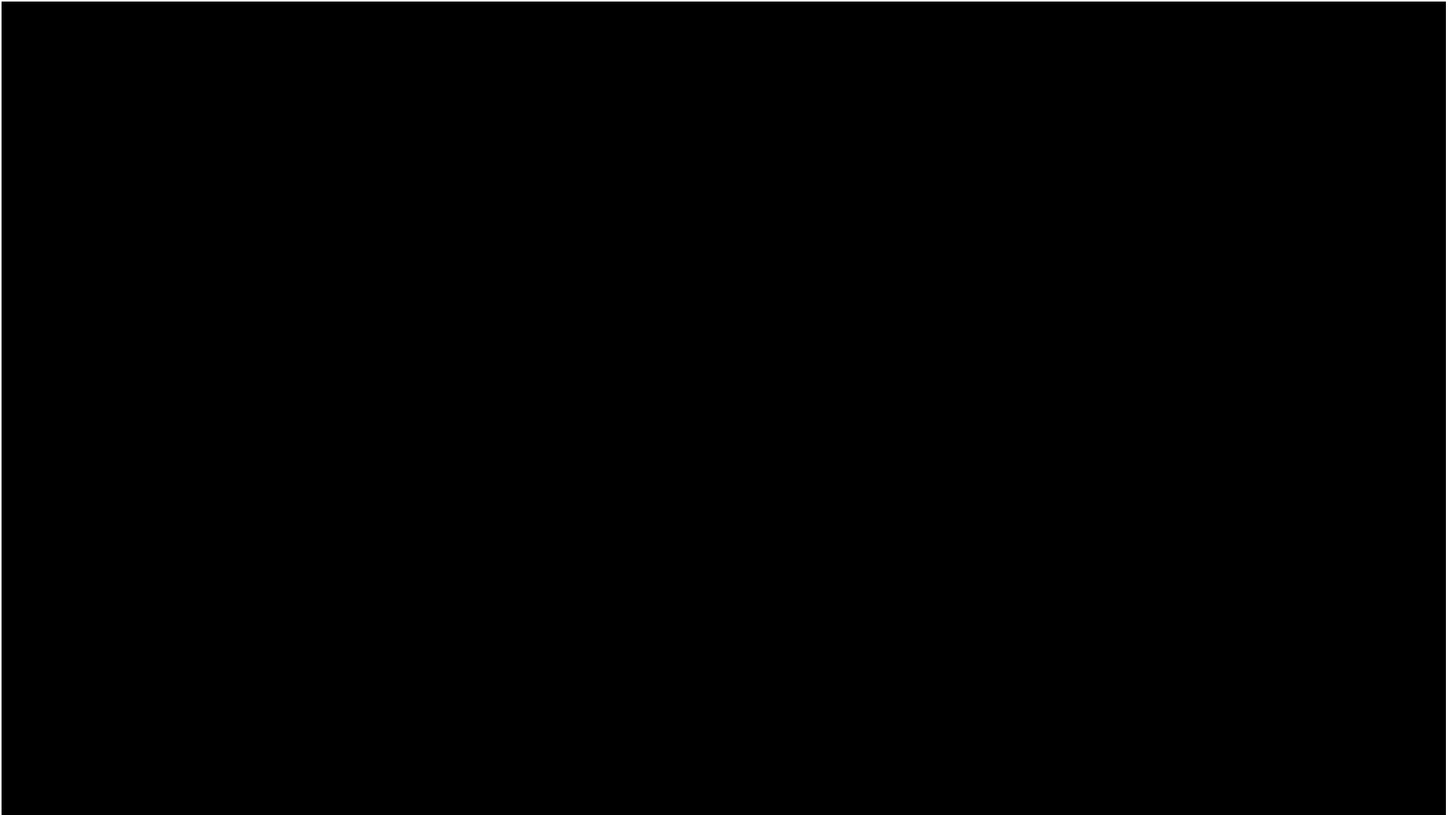
EXHIBITS AND ATTACHMENTS



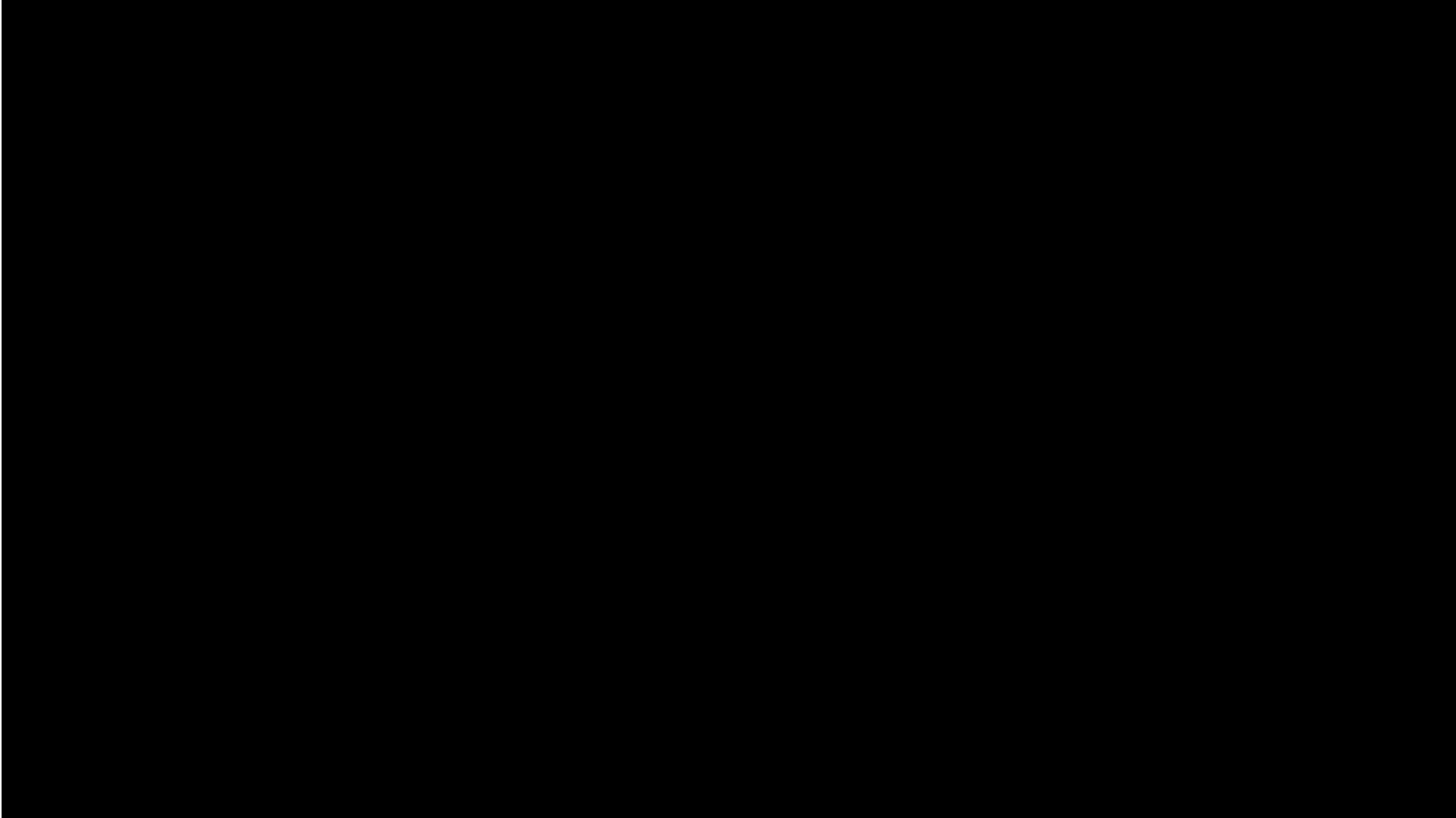
EXHIBITS AND ATTACHMENTS



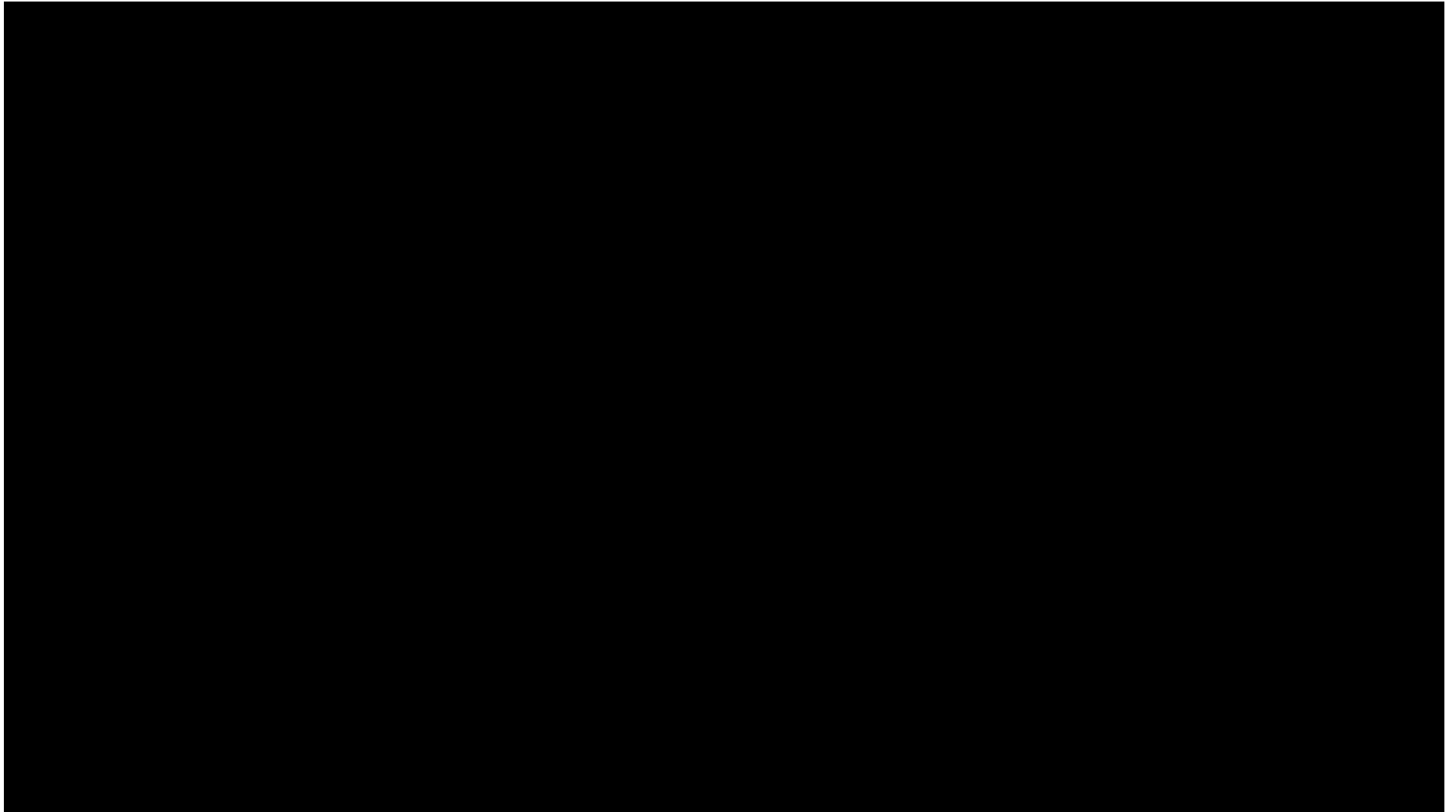
EXHIBITS AND ATTACHMENTS



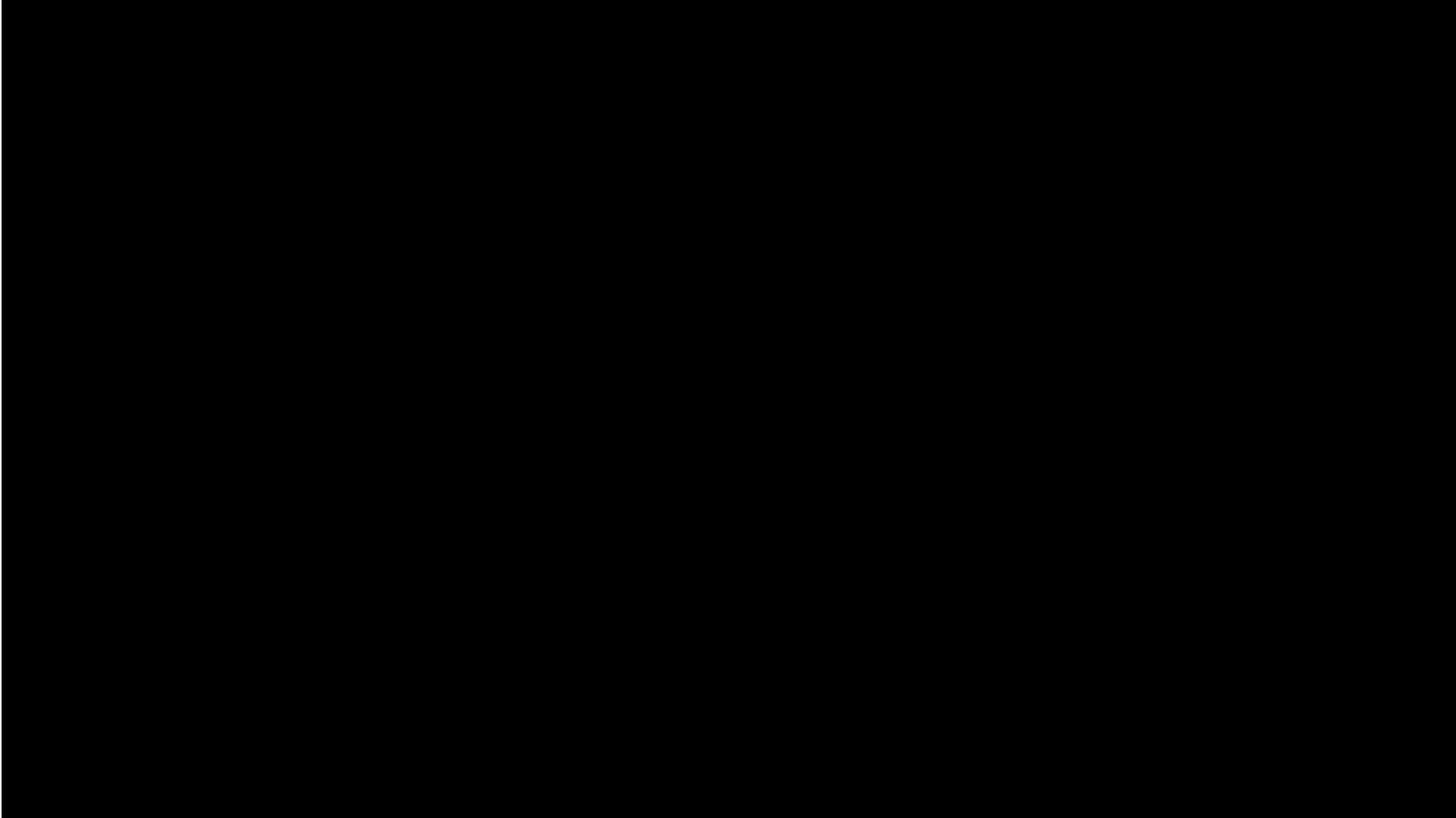
EXHIBITS AND ATTACHMENTS



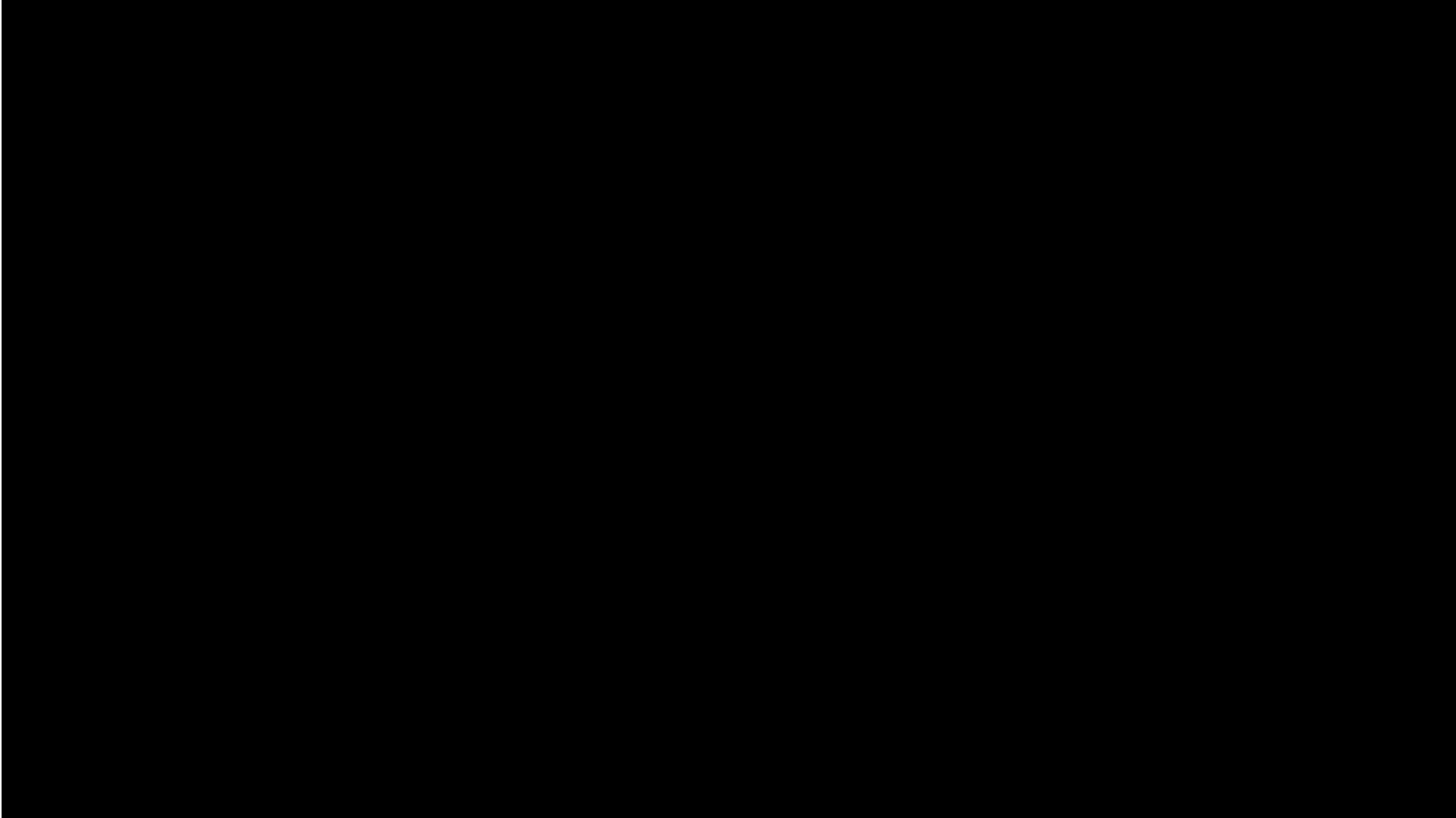
EXHIBITS AND ATTACHMENTS



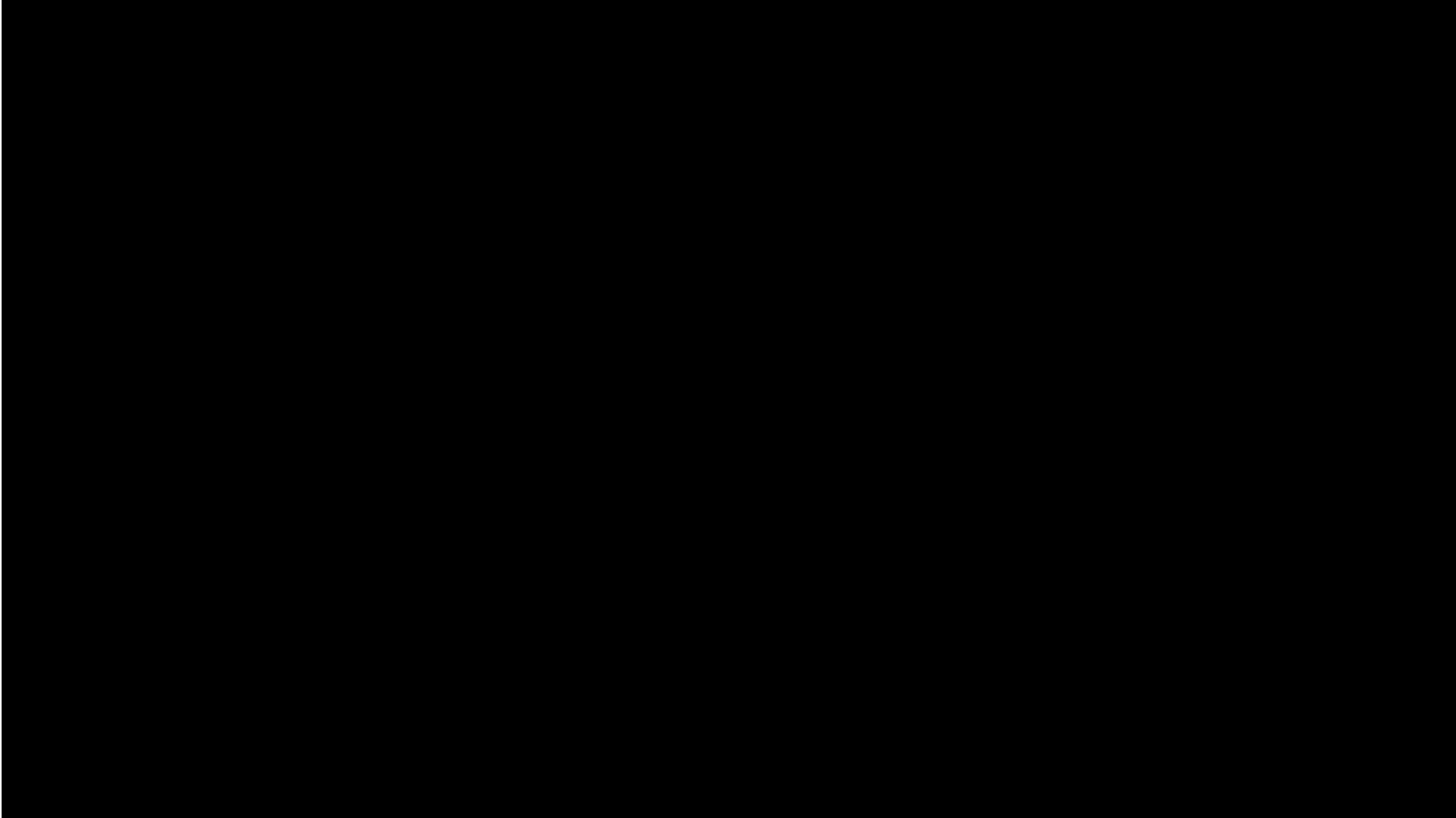
EXHIBITS AND ATTACHMENTS



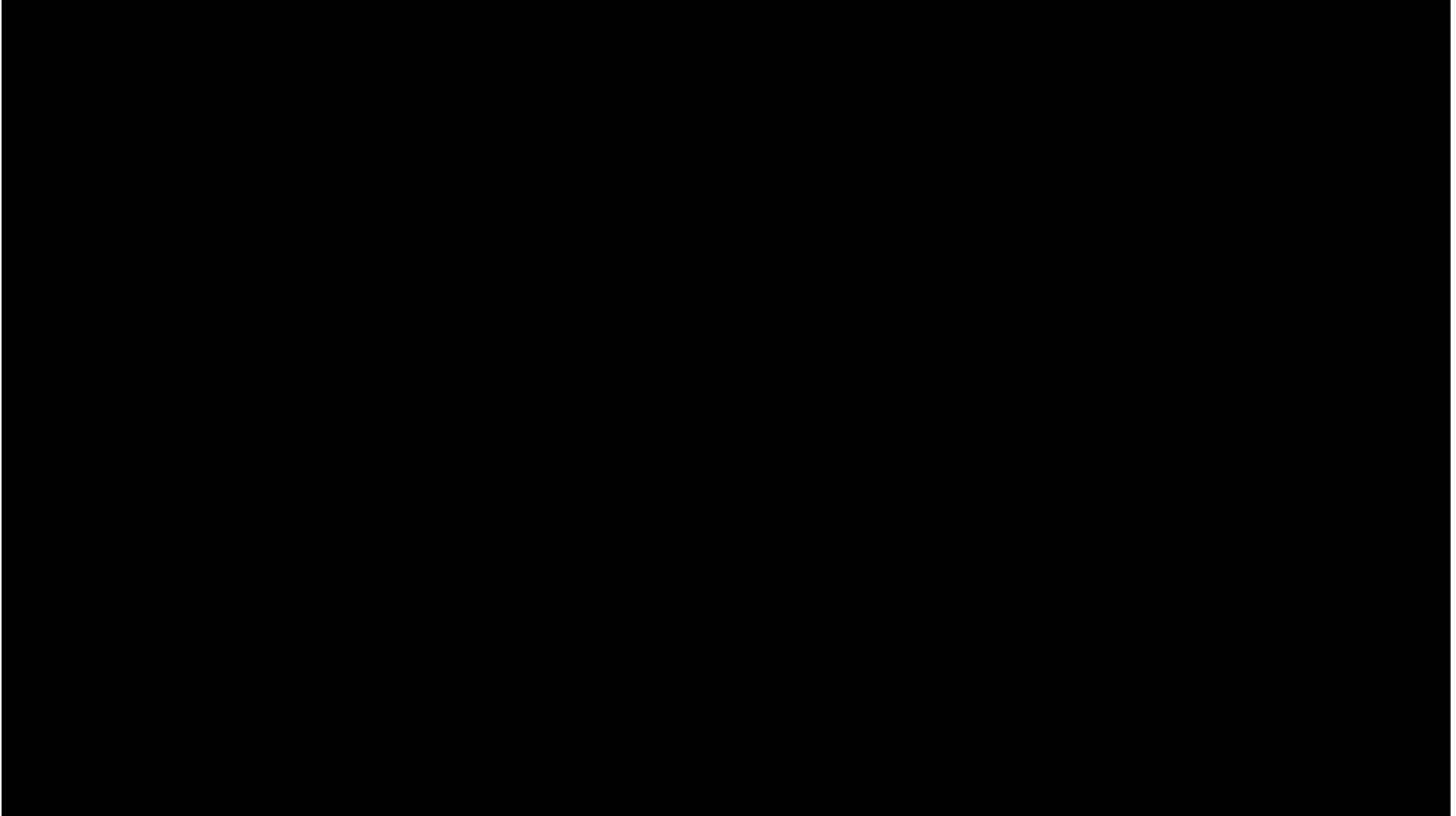
EXHIBITS AND ATTACHMENTS



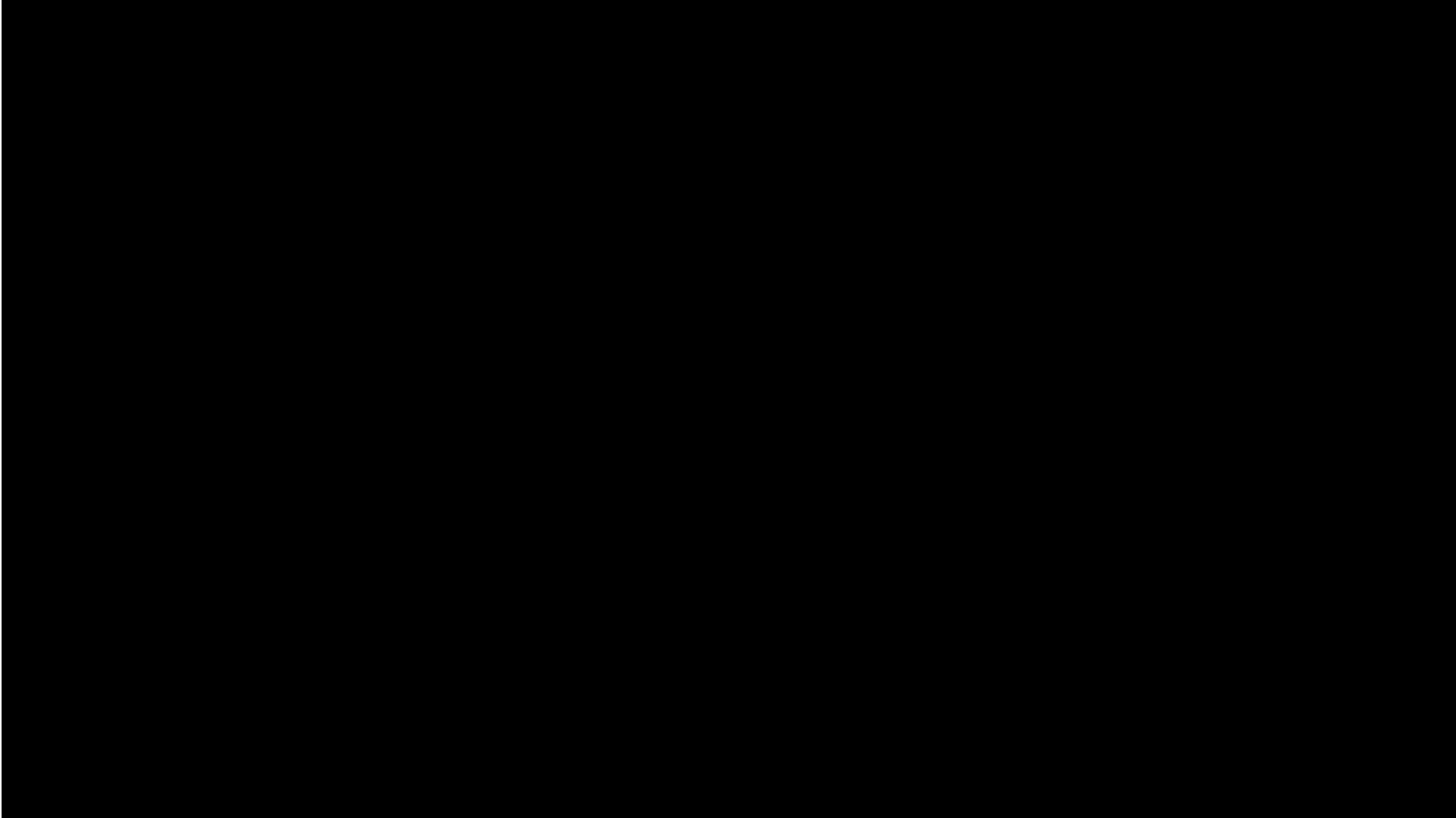
EXHIBITS AND ATTACHMENTS



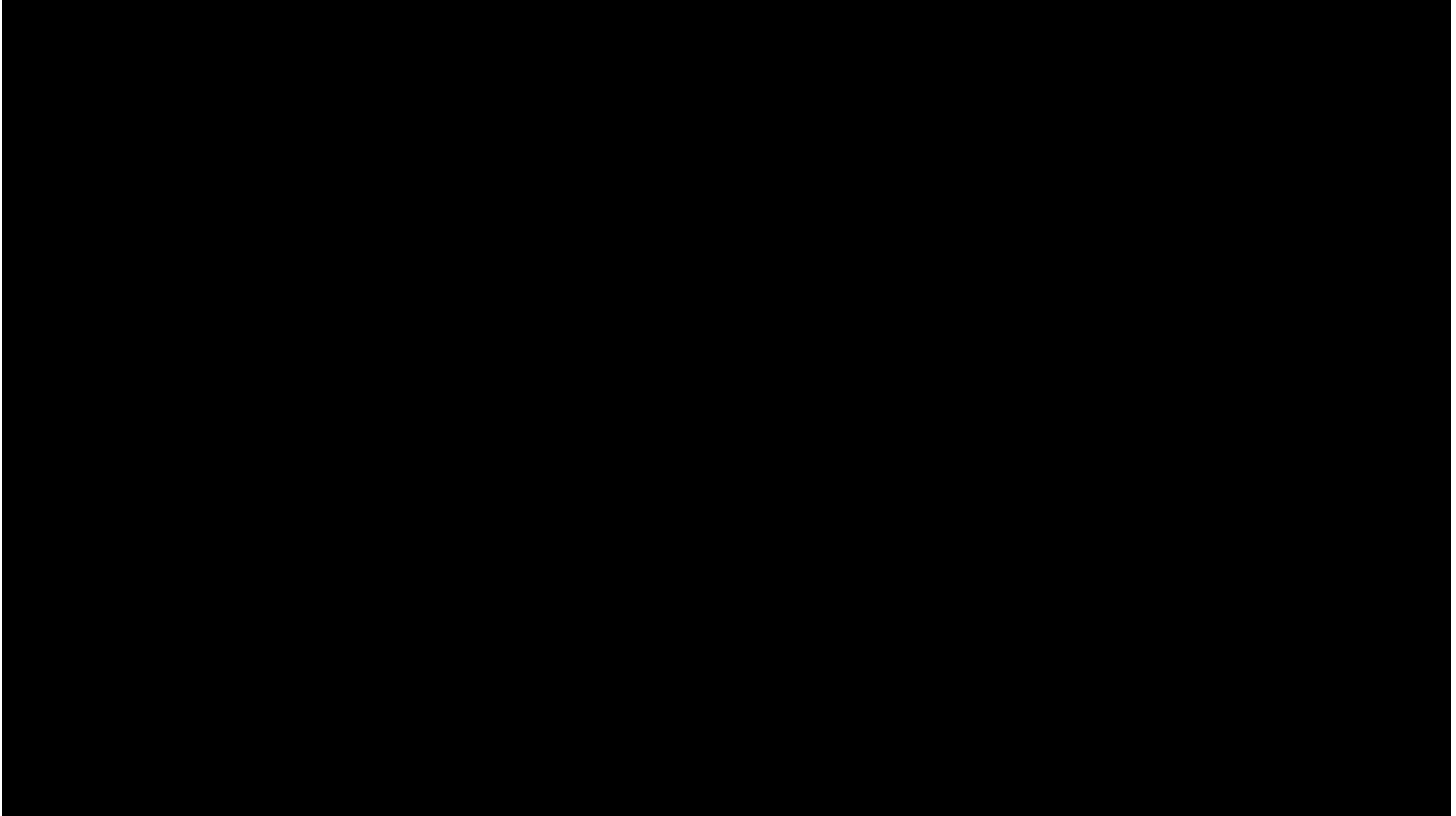
EXHIBITS AND ATTACHMENTS



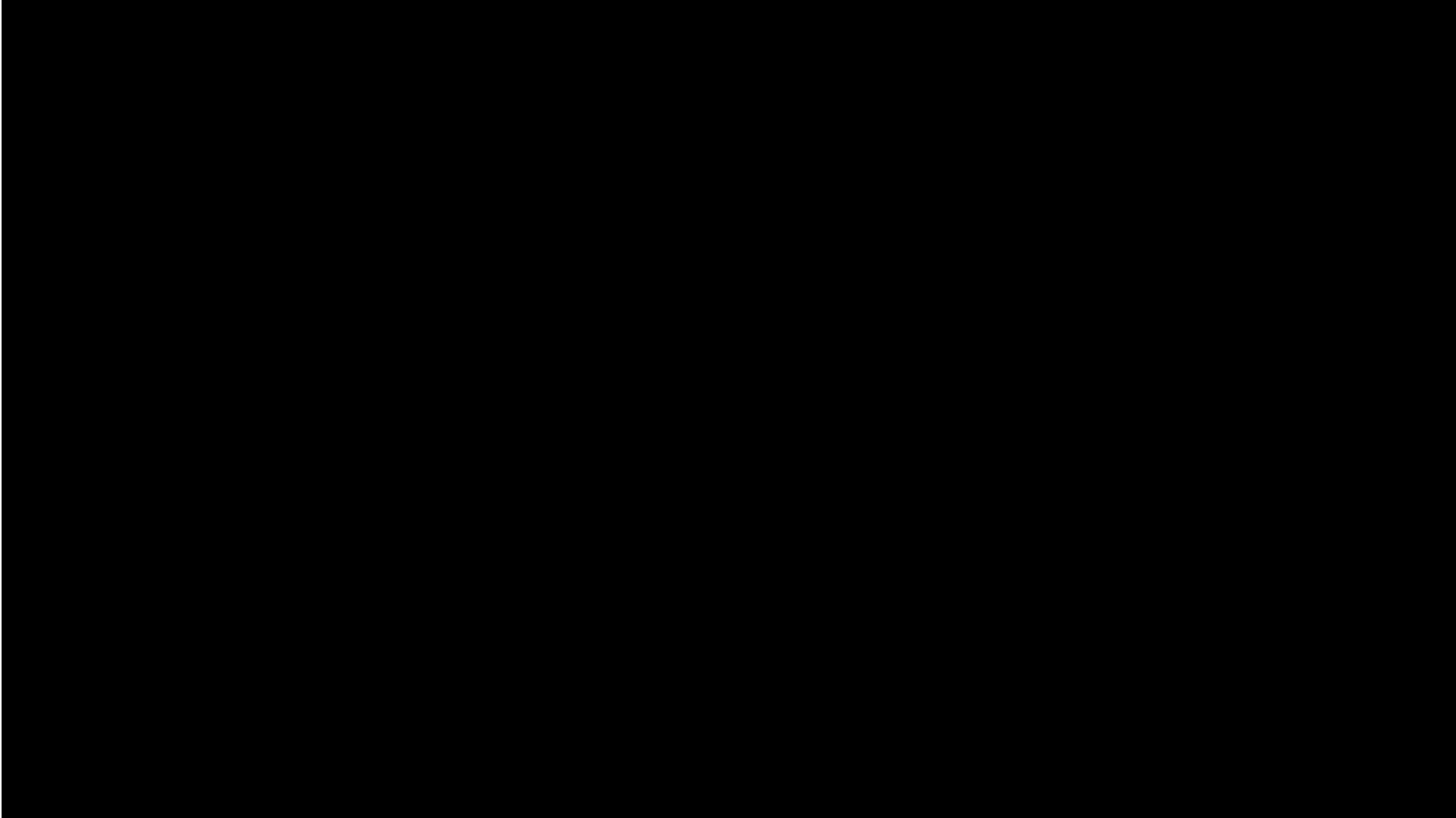
EXHIBITS AND ATTACHMENTS



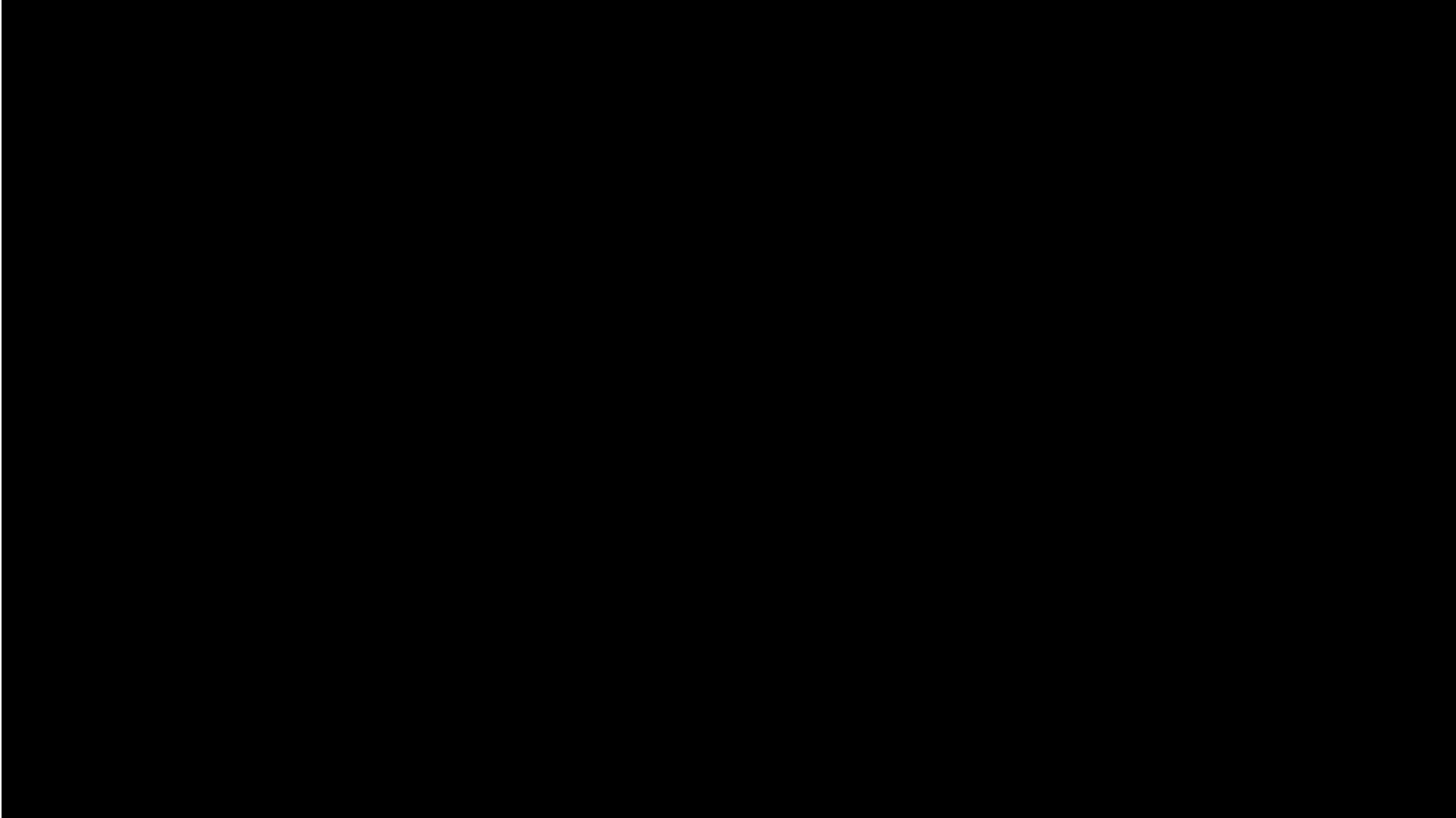
EXHIBITS AND ATTACHMENTS



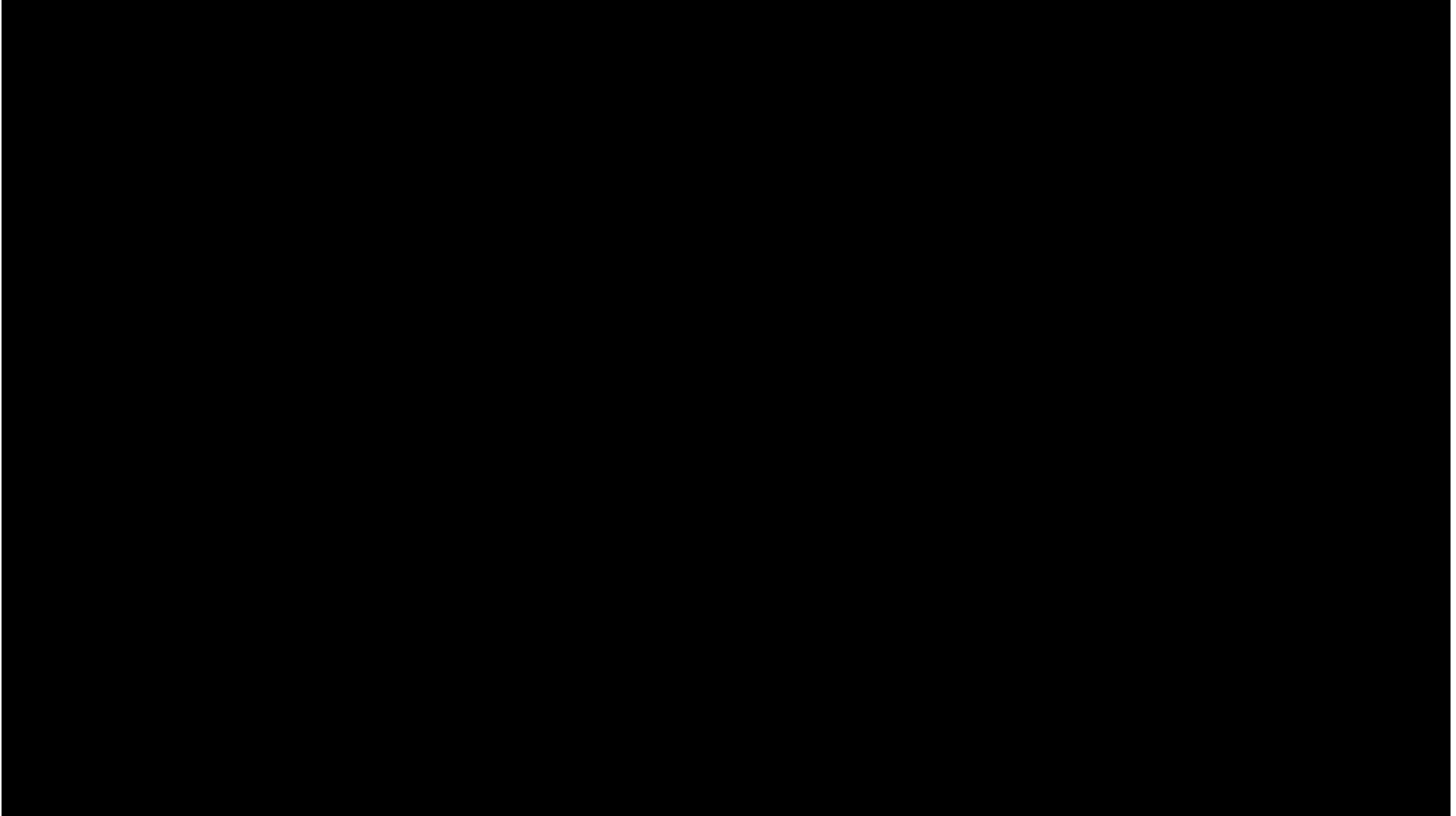
EXHIBITS AND ATTACHMENTS



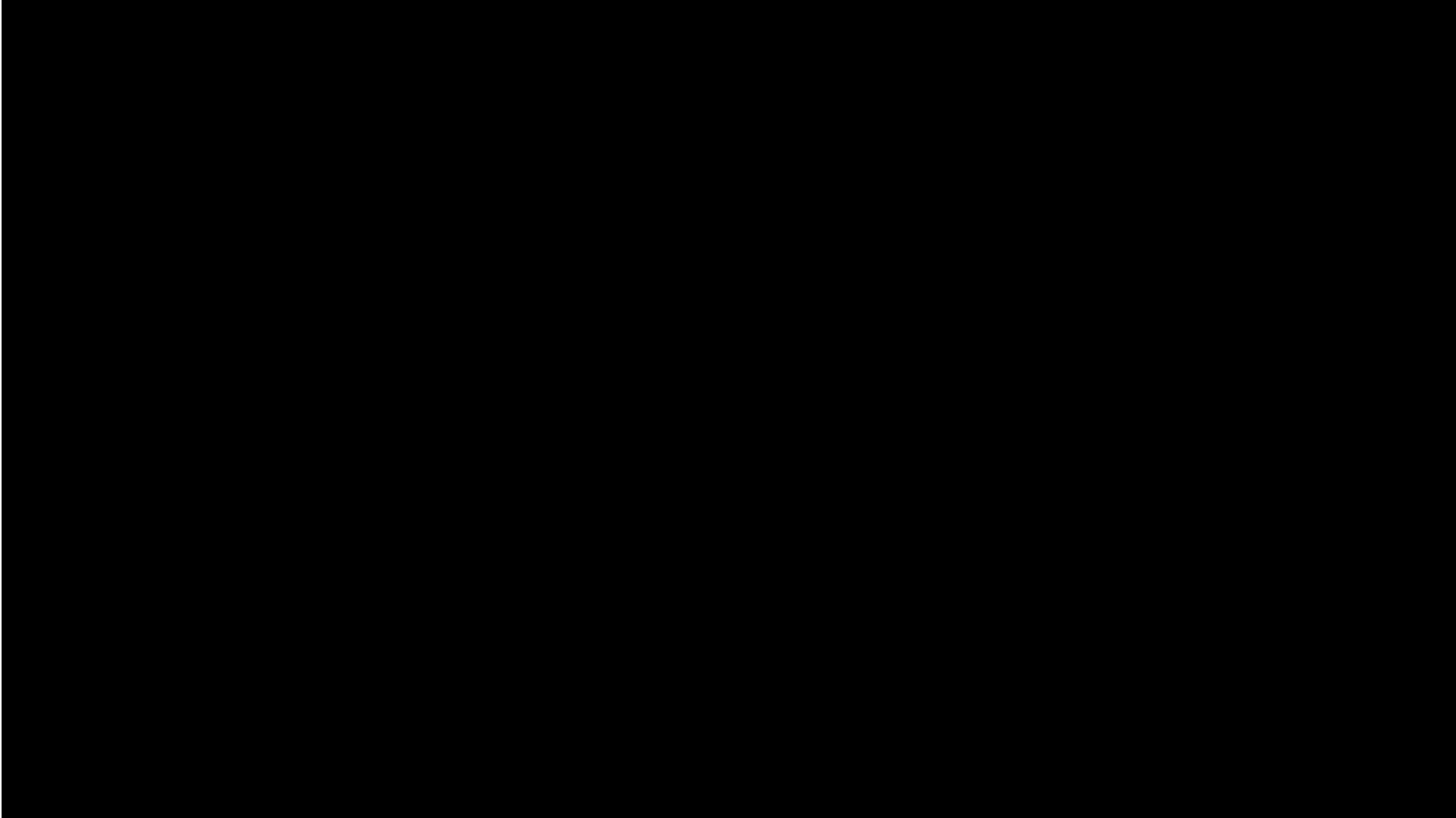
EXHIBITS AND ATTACHMENTS



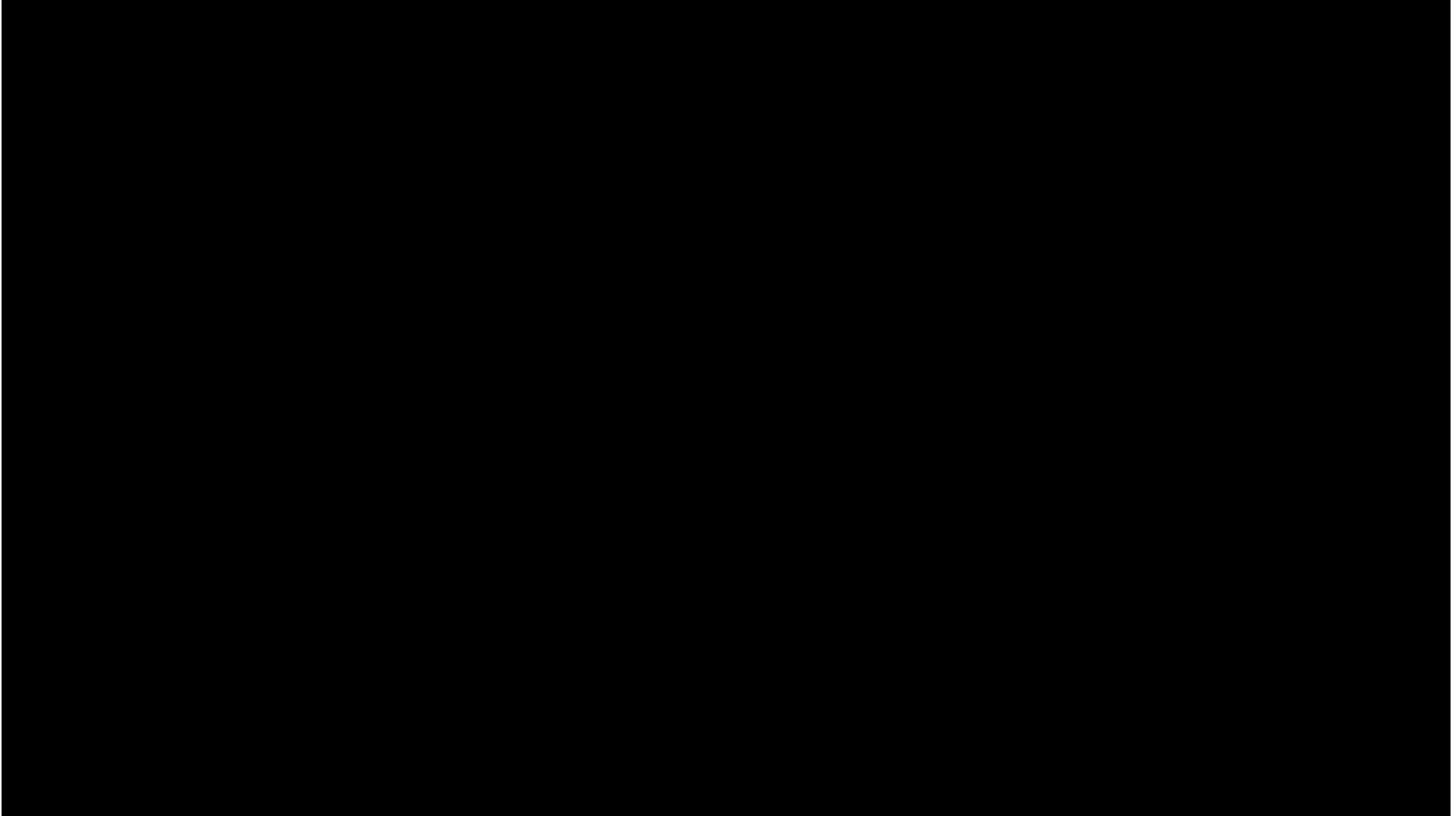
EXHIBITS AND ATTACHMENTS



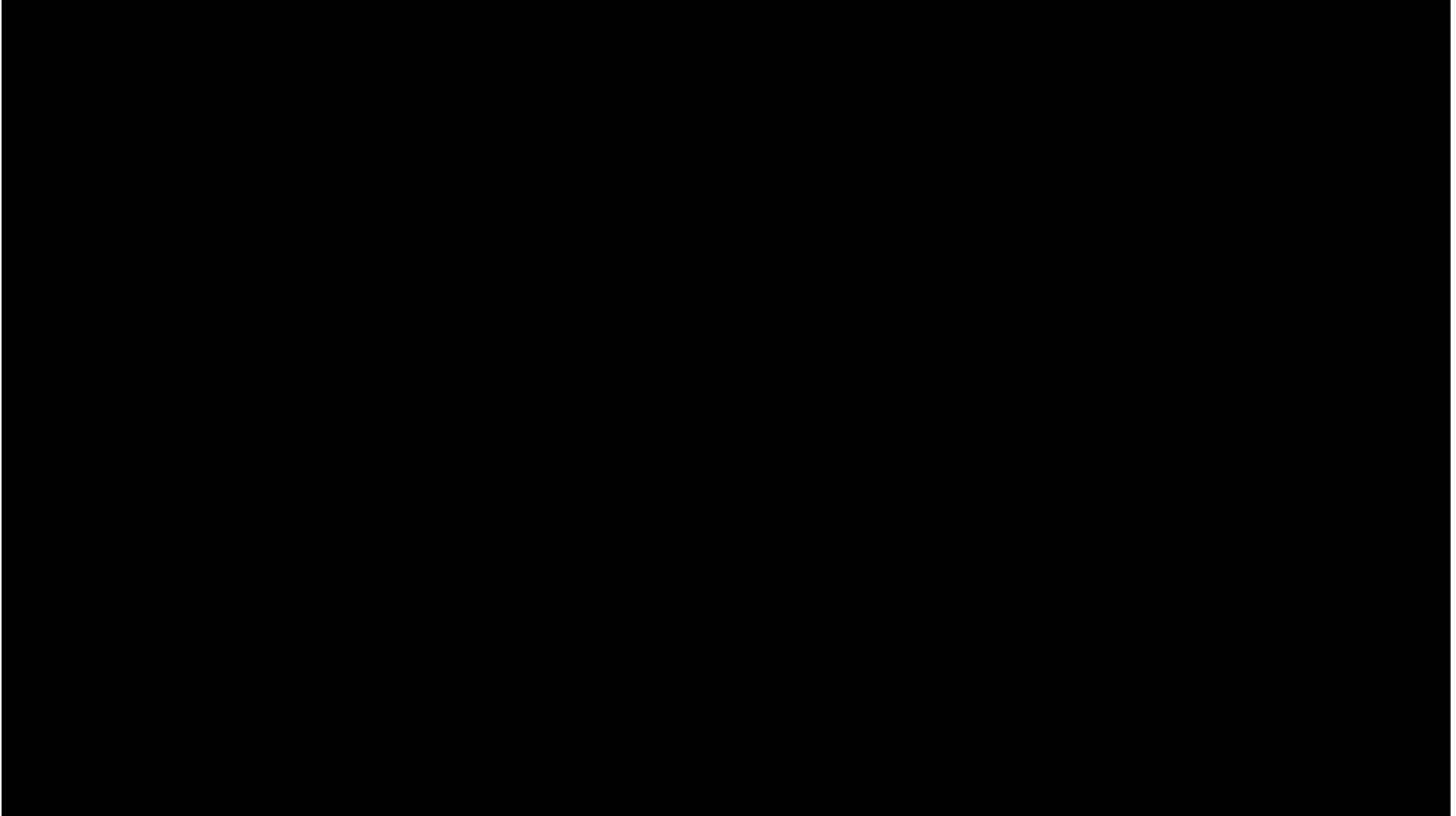
EXHIBITS AND ATTACHMENTS



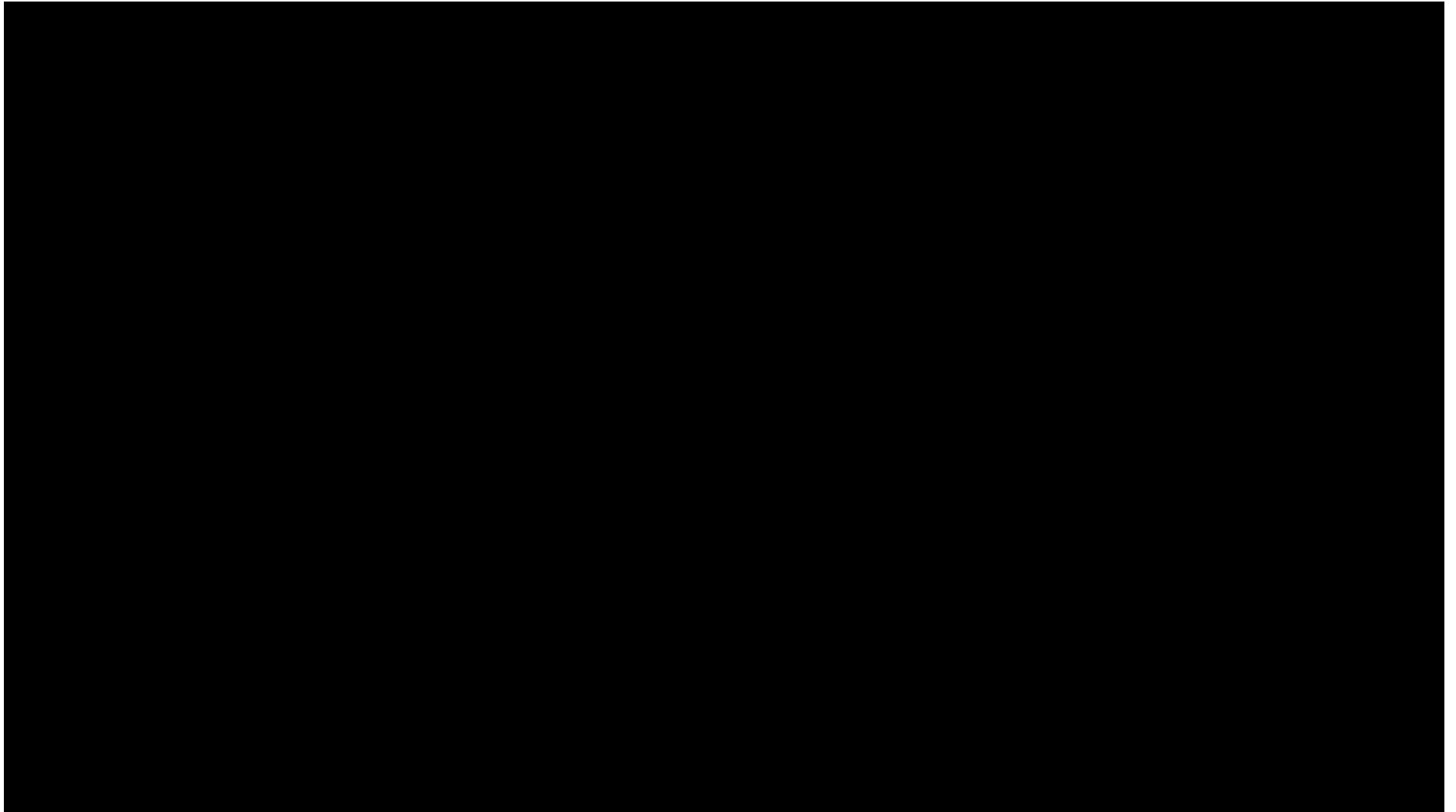
EXHIBITS AND ATTACHMENTS



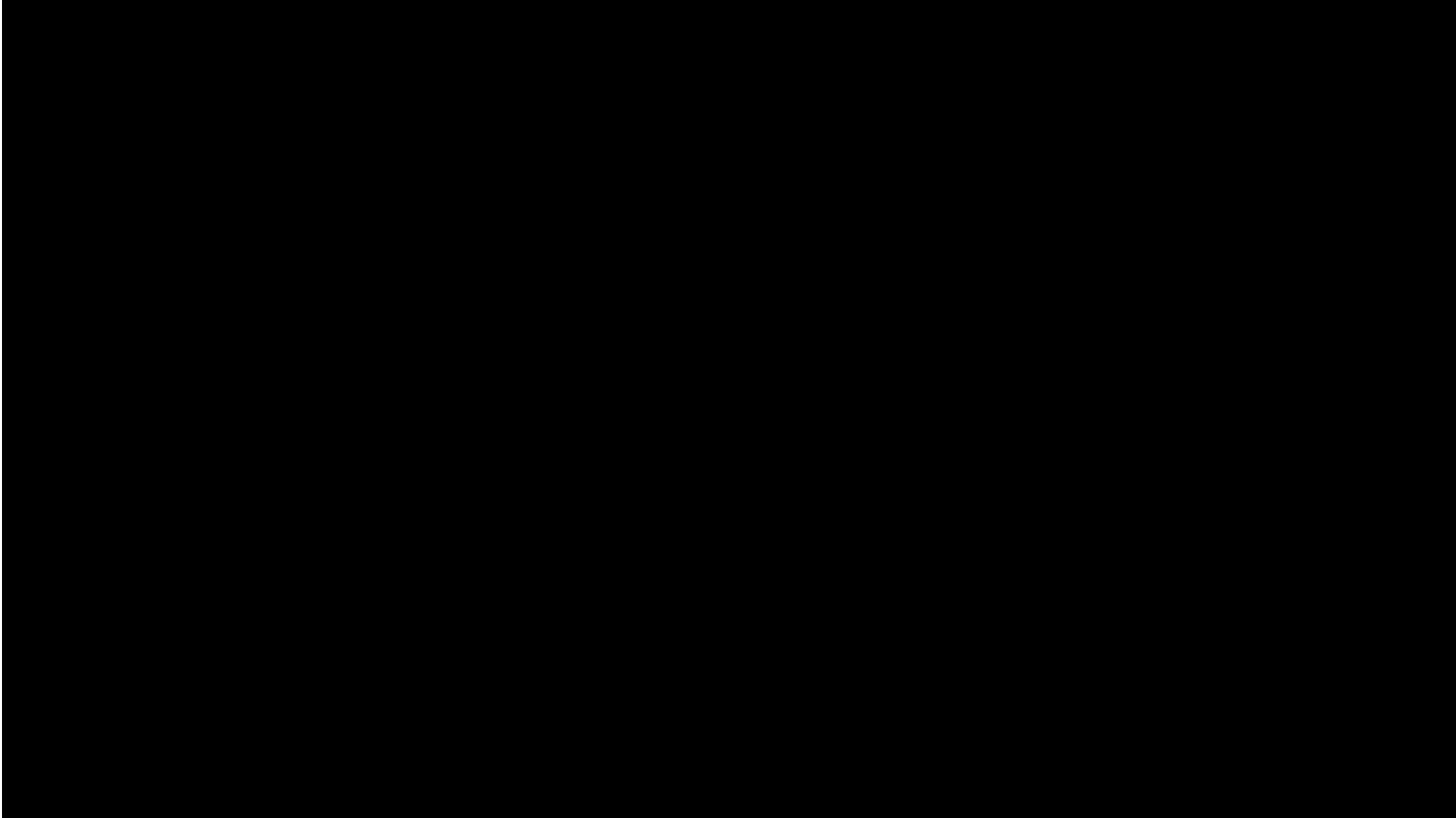
EXHIBITS AND ATTACHMENTS



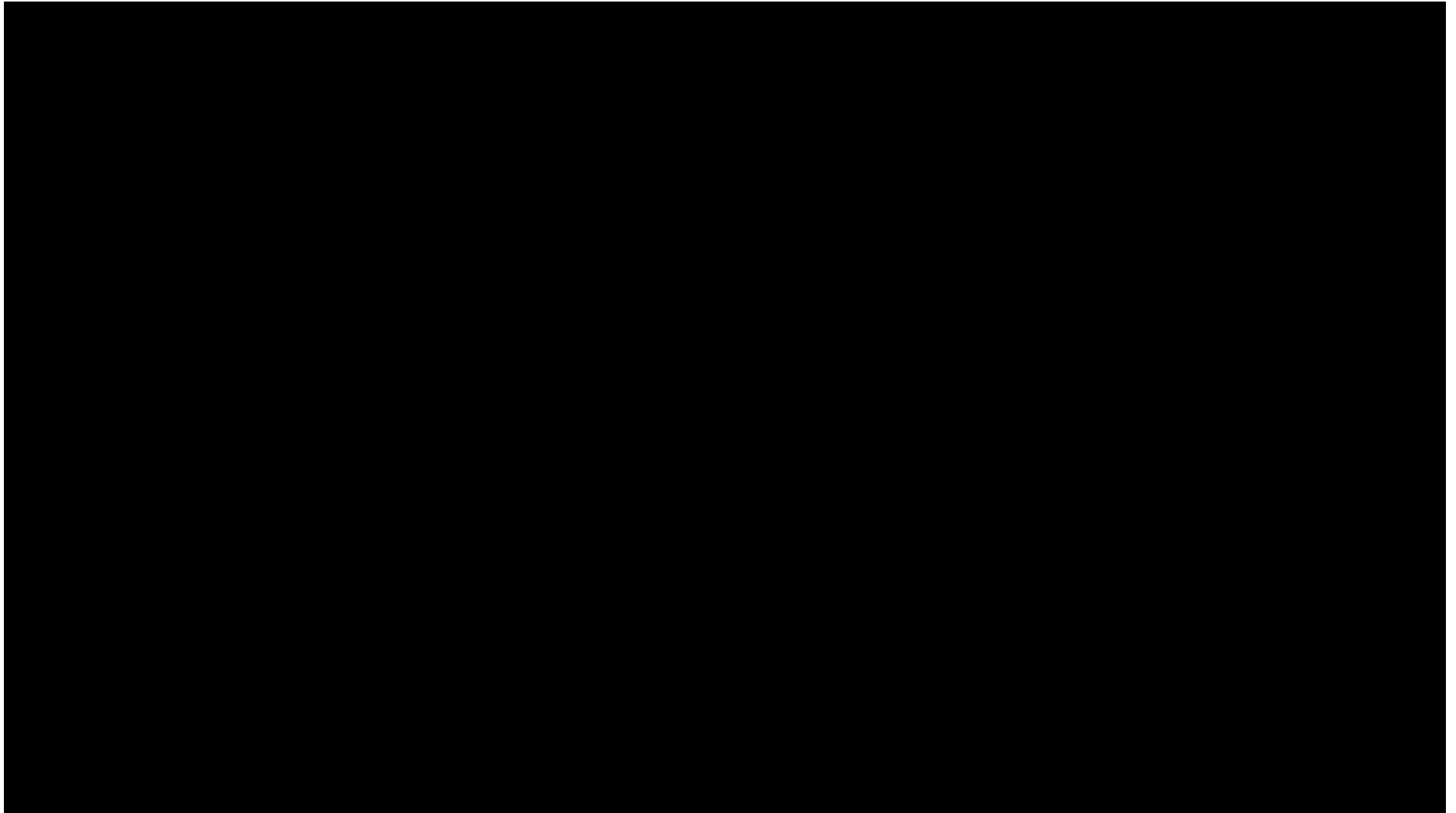
EXHIBITS AND ATTACHMENTS



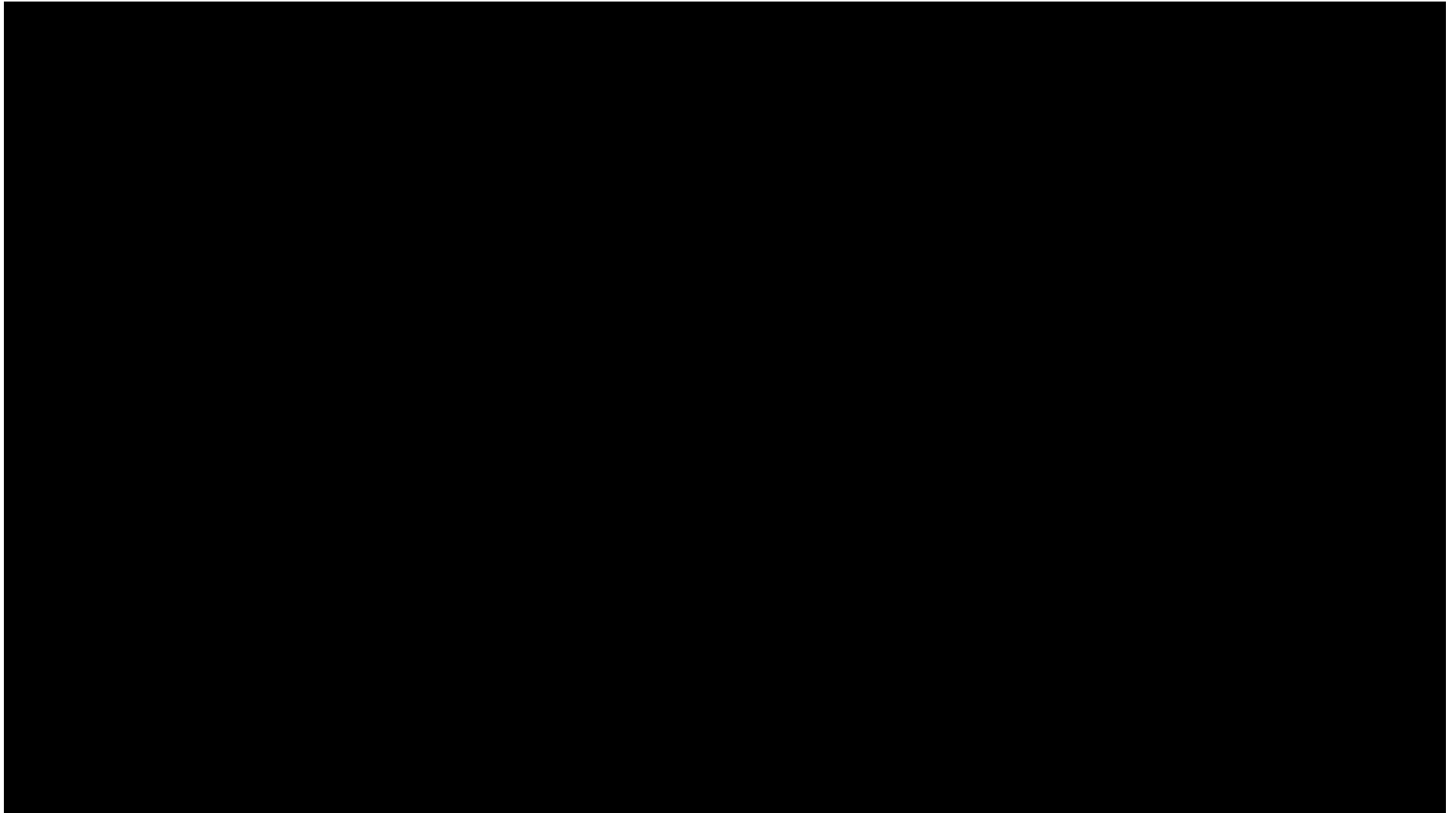
EXHIBITS AND ATTACHMENTS



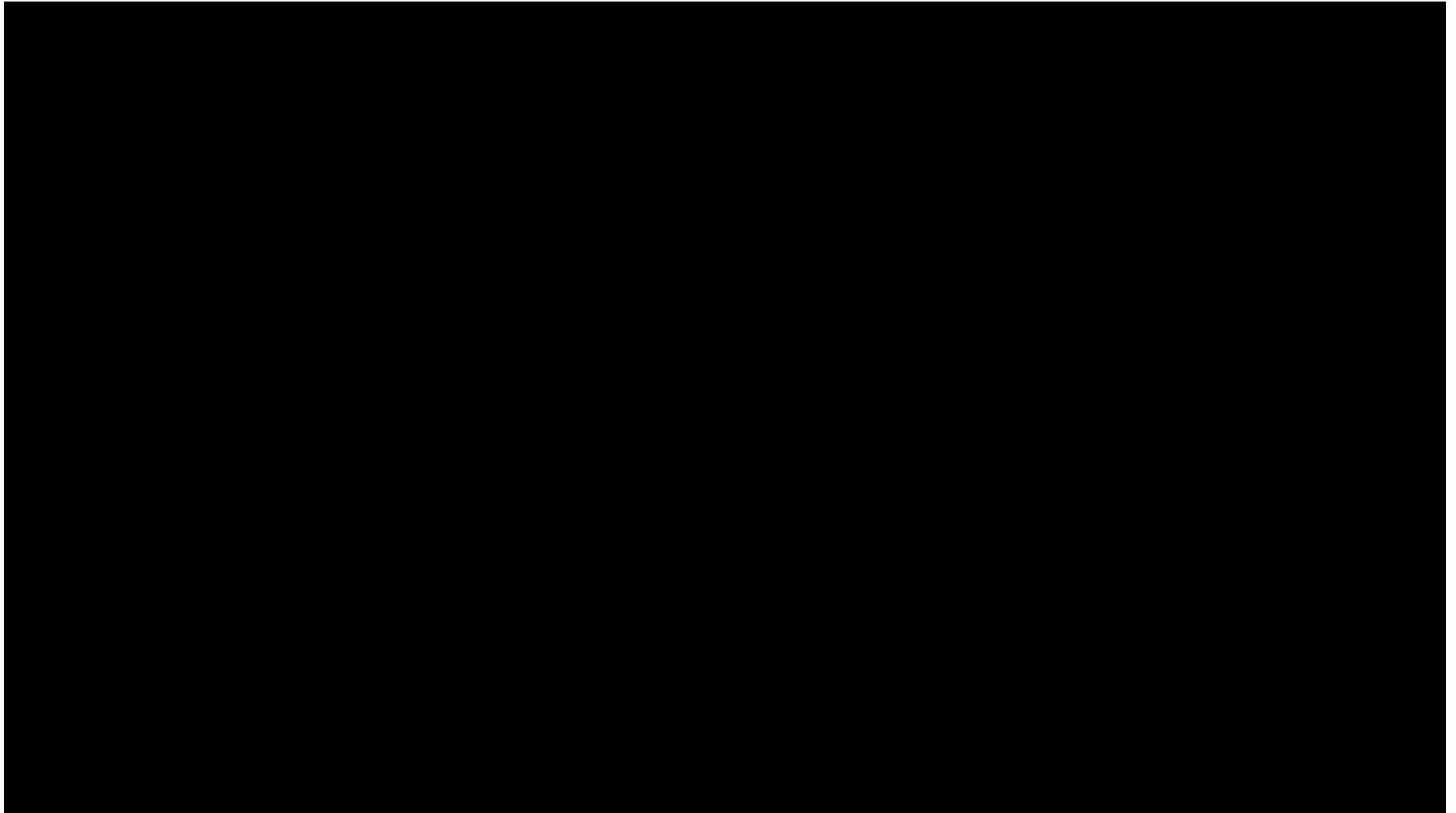
EXHIBITS AND ATTACHMENTS



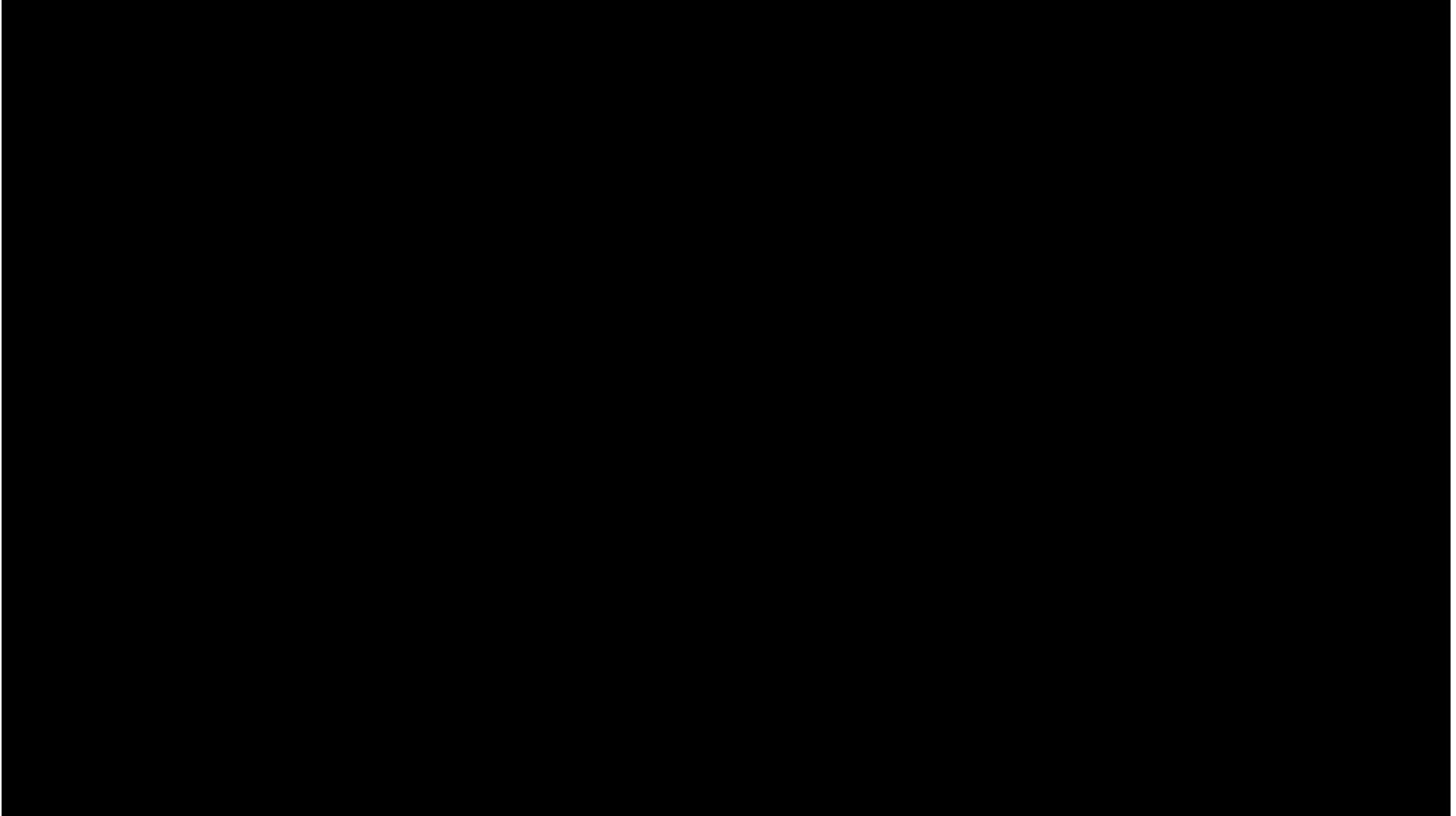
EXHIBITS AND ATTACHMENTS



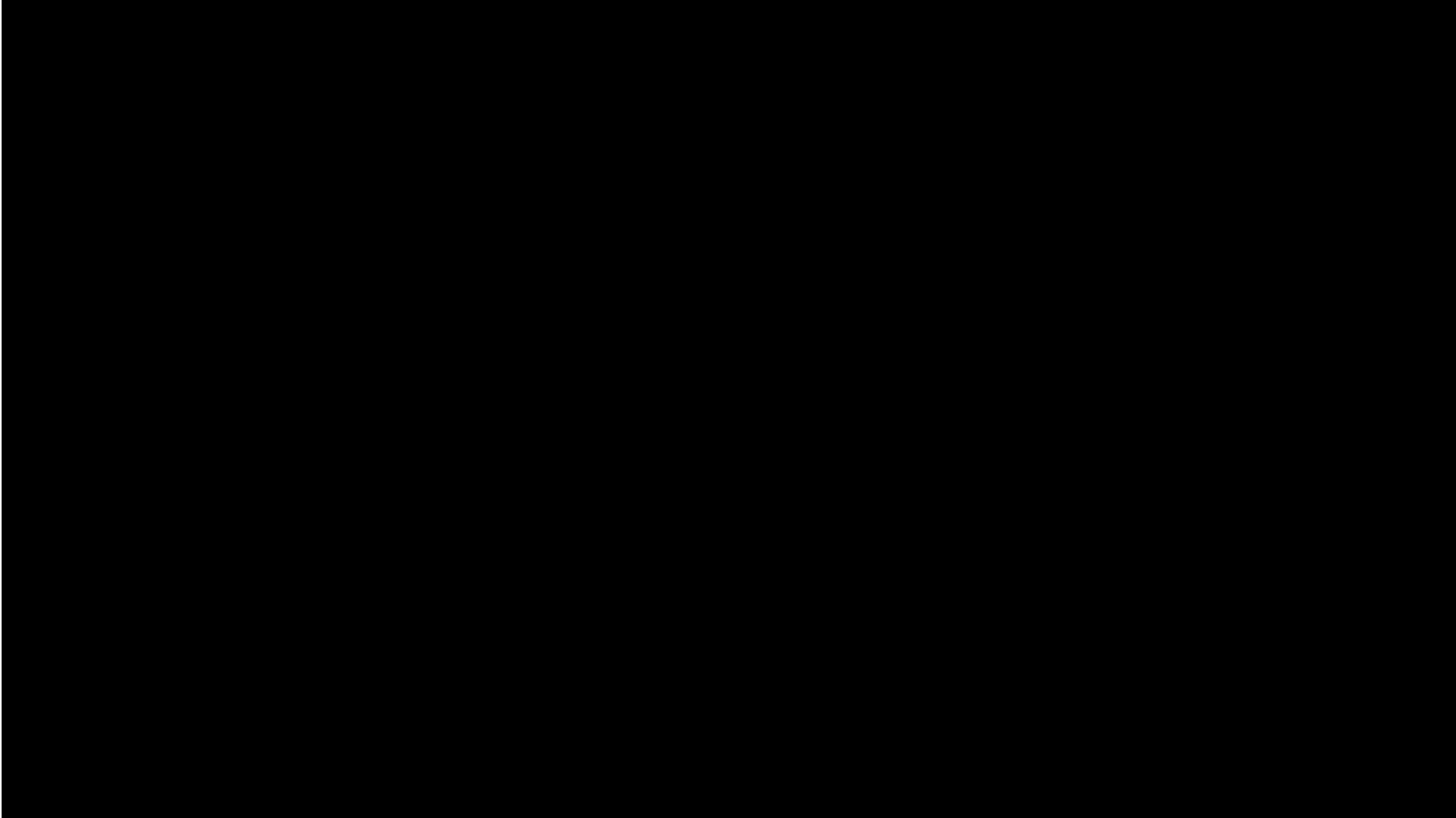
EXHIBITS AND ATTACHMENTS



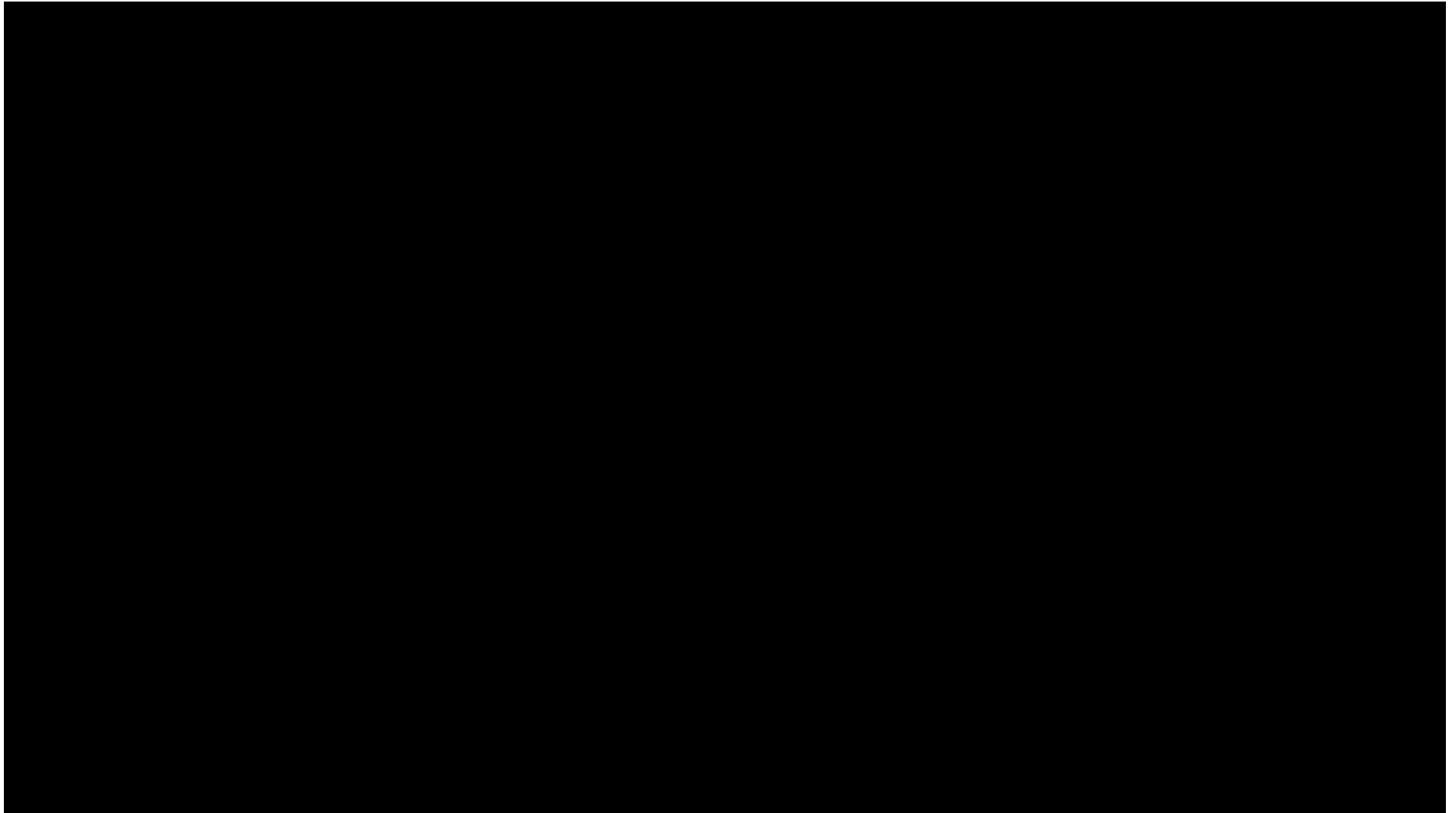
EXHIBITS AND ATTACHMENTS



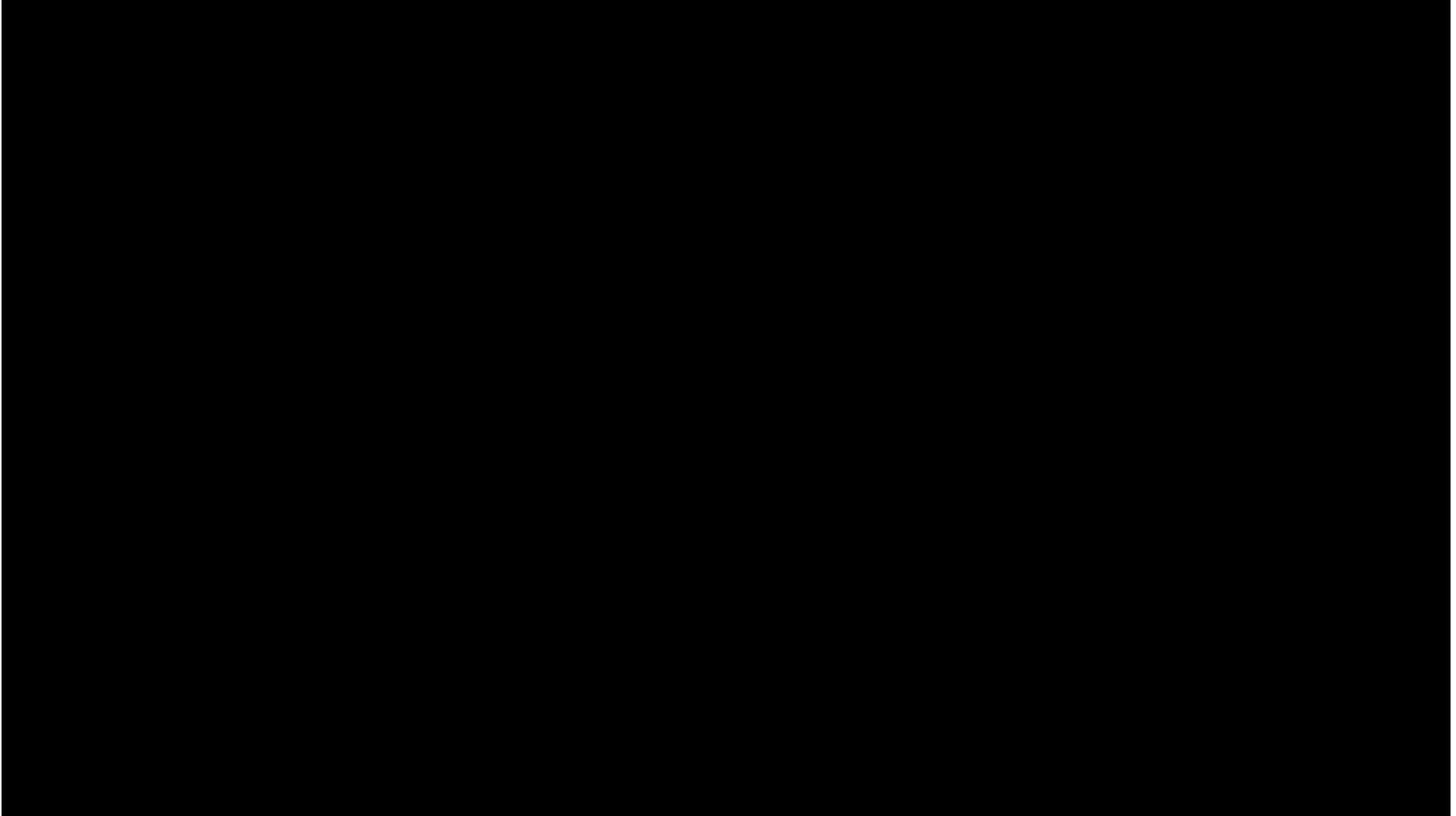
EXHIBITS AND ATTACHMENTS



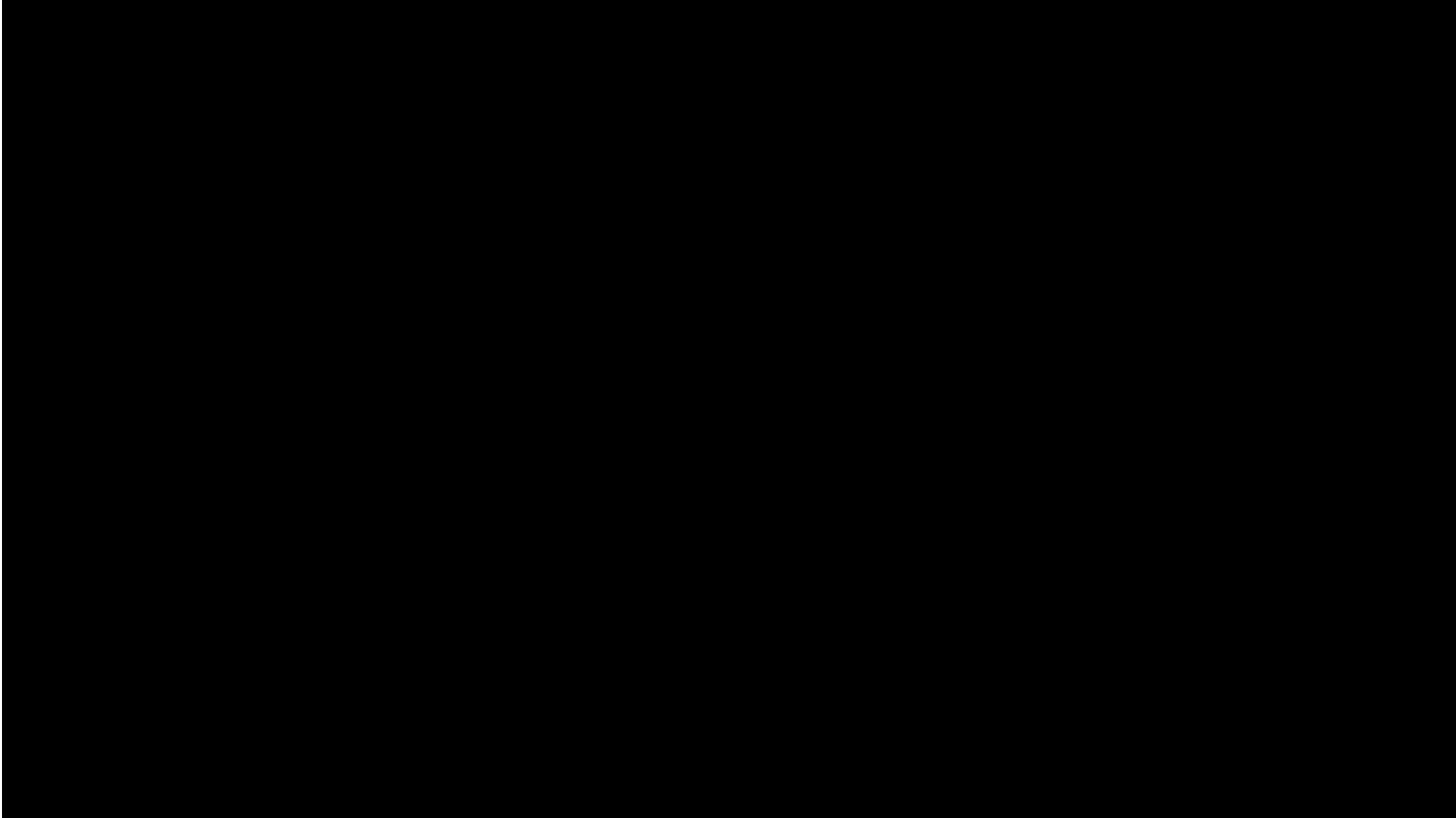
EXHIBITS AND ATTACHMENTS



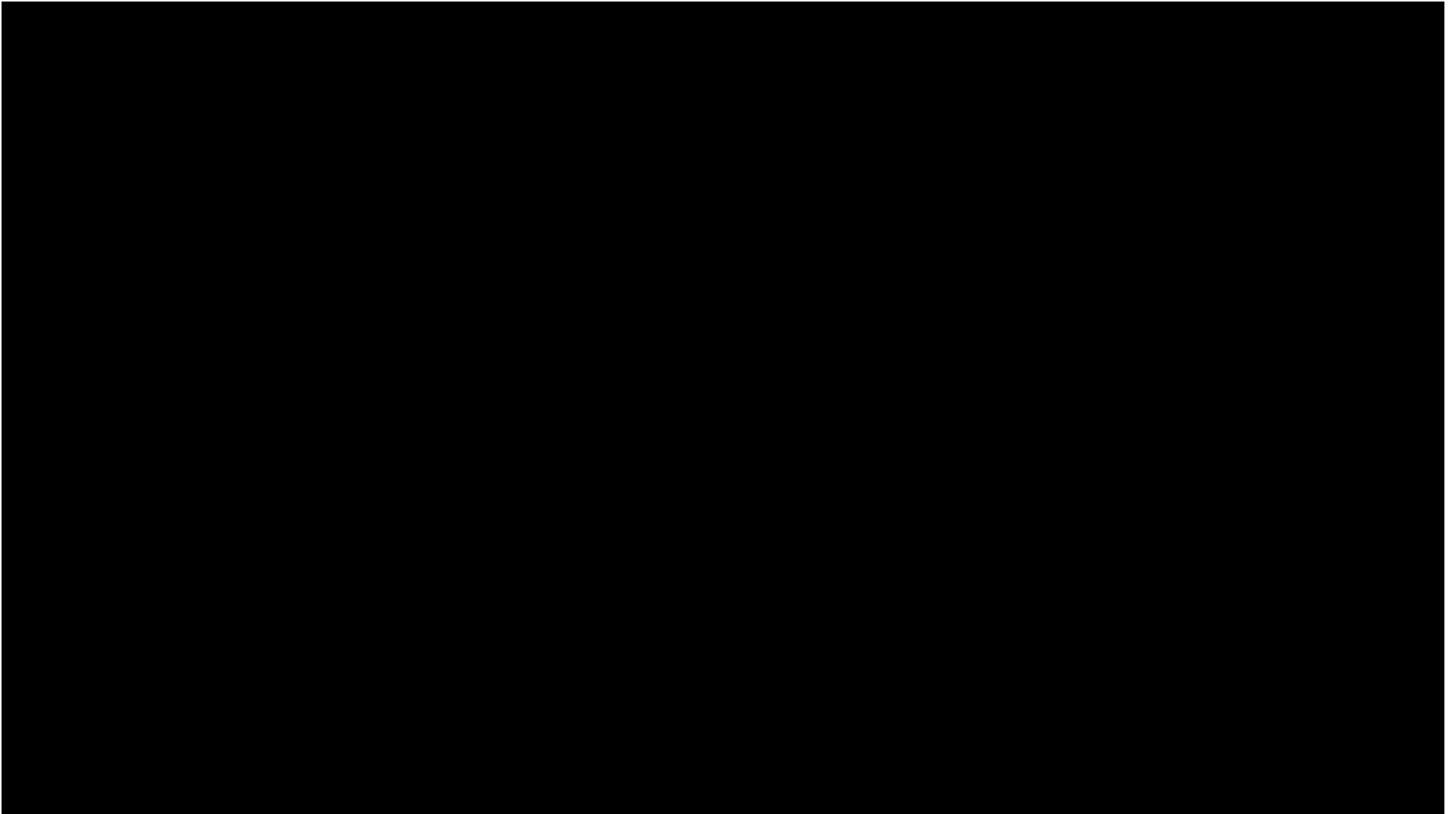
EXHIBITS AND ATTACHMENTS



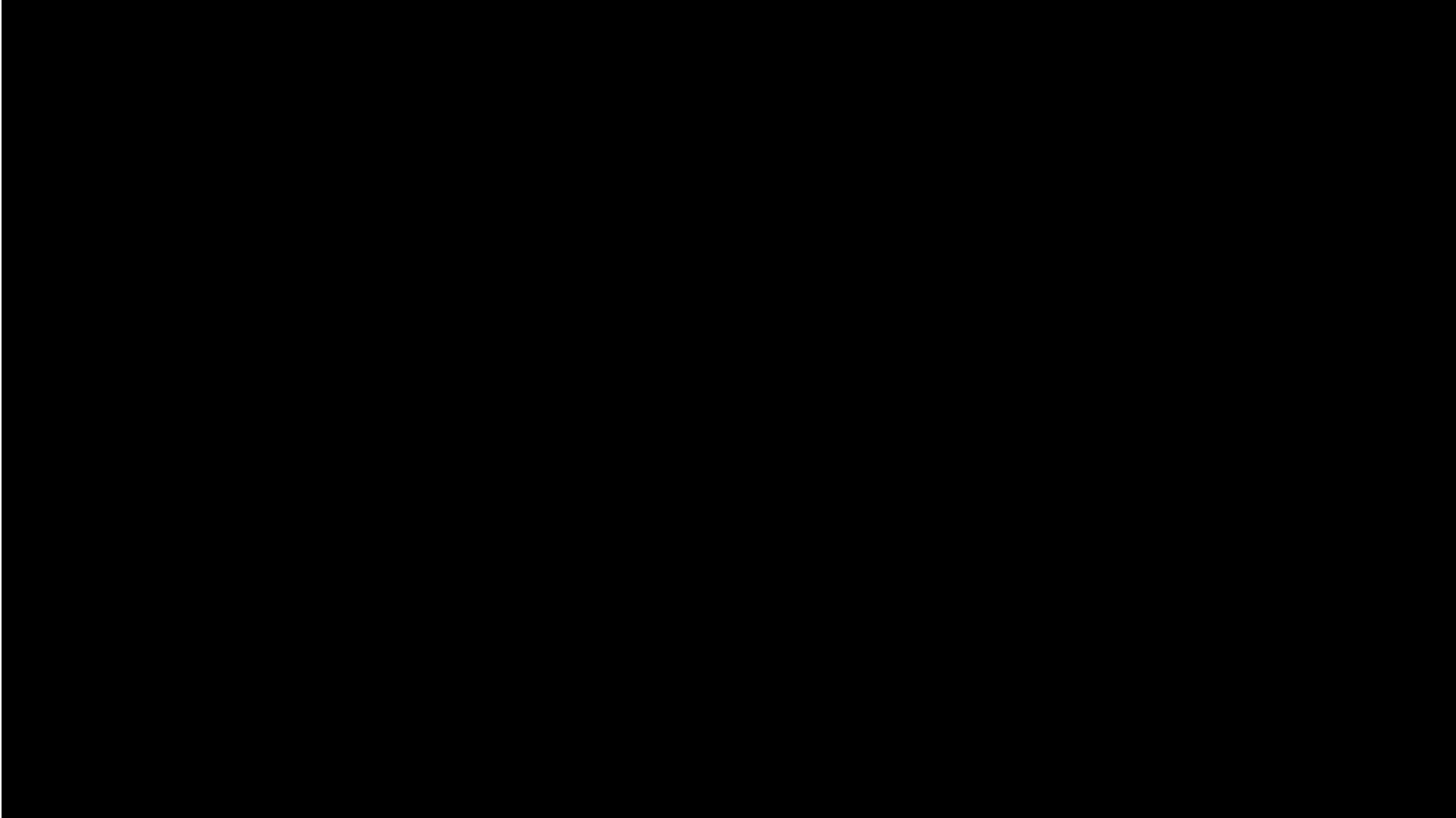
EXHIBITS AND ATTACHMENTS



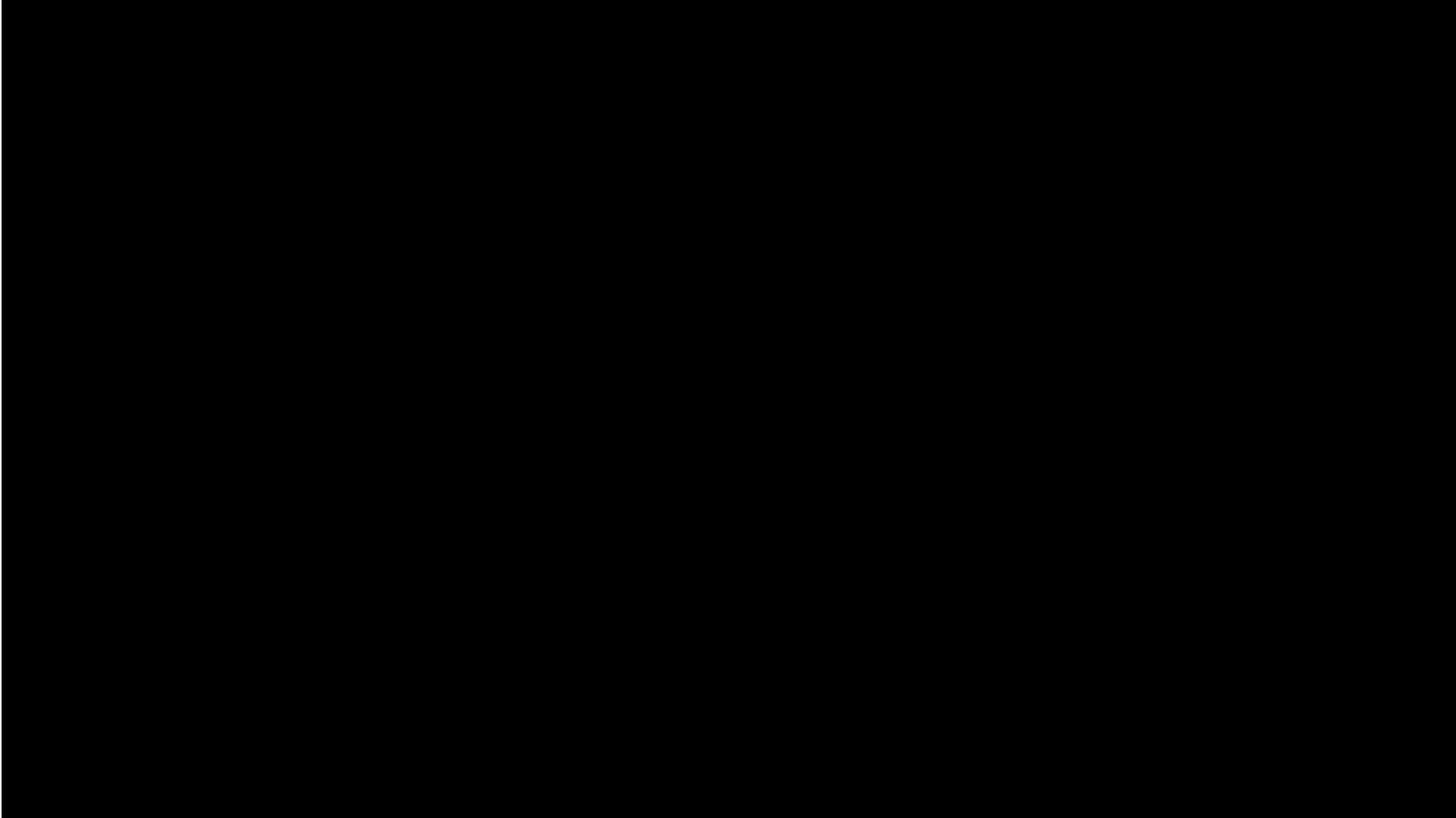
EXHIBITS AND ATTACHMENTS



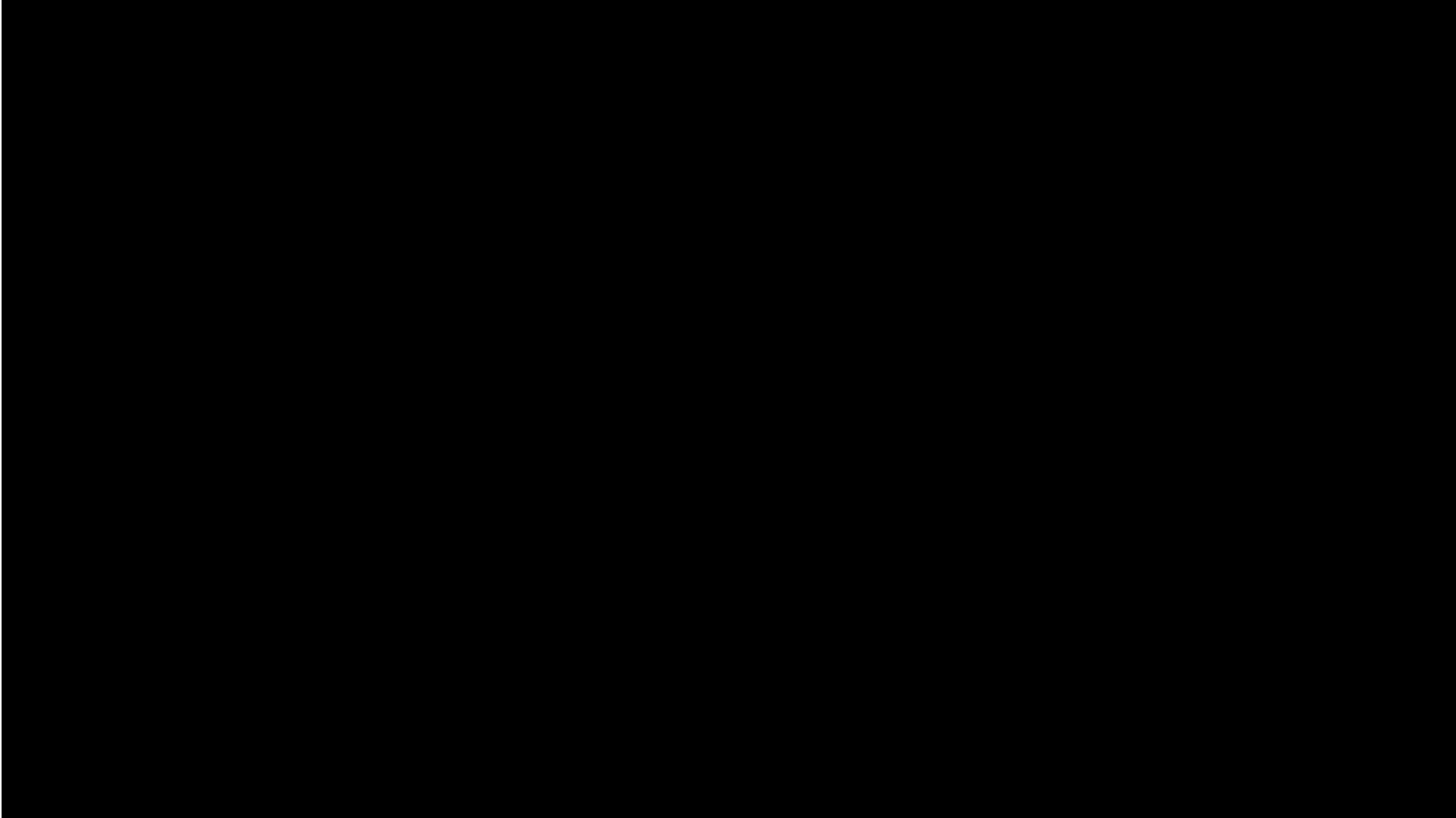
EXHIBITS AND ATTACHMENTS



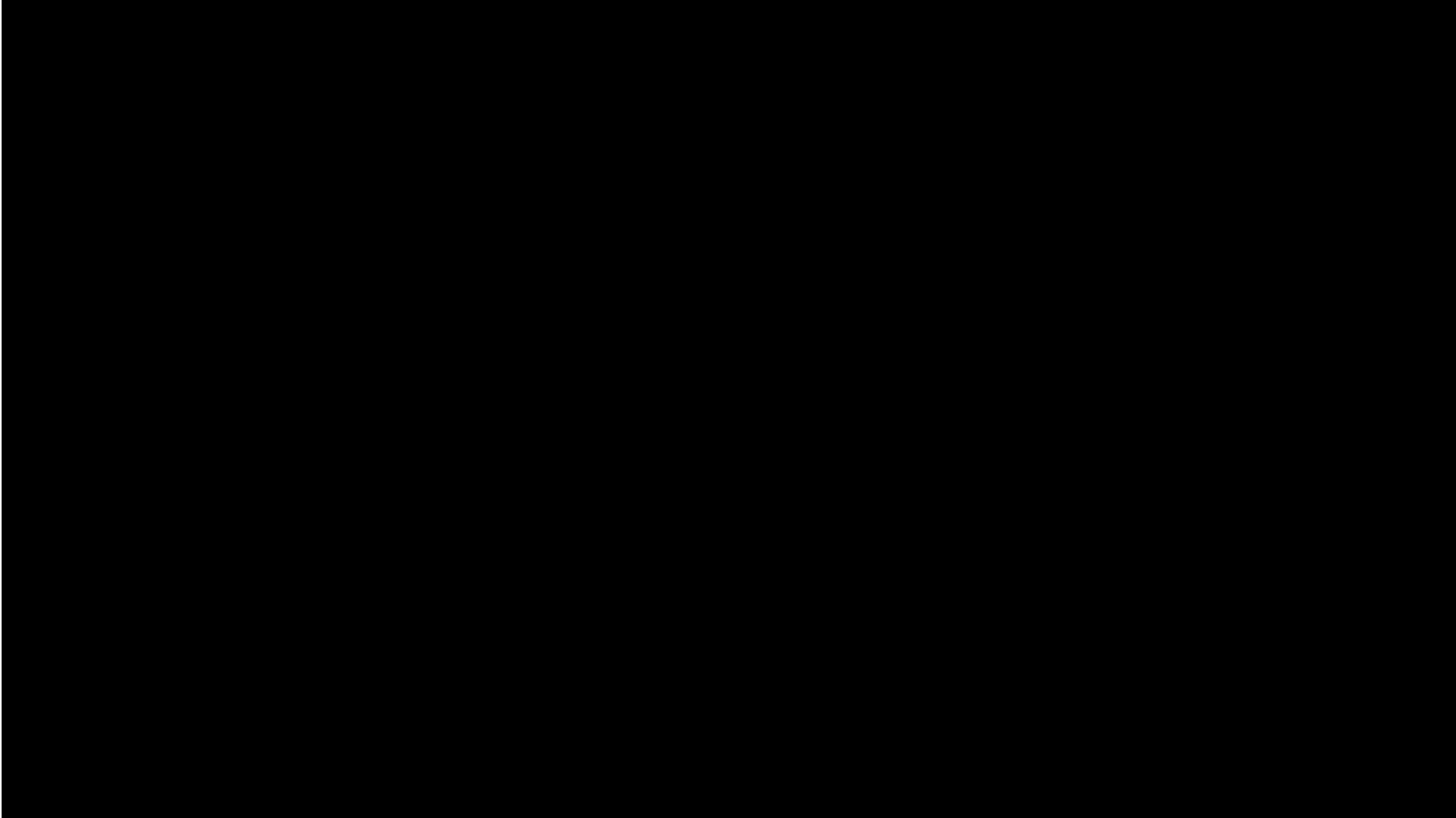
EXHIBITS AND ATTACHMENTS



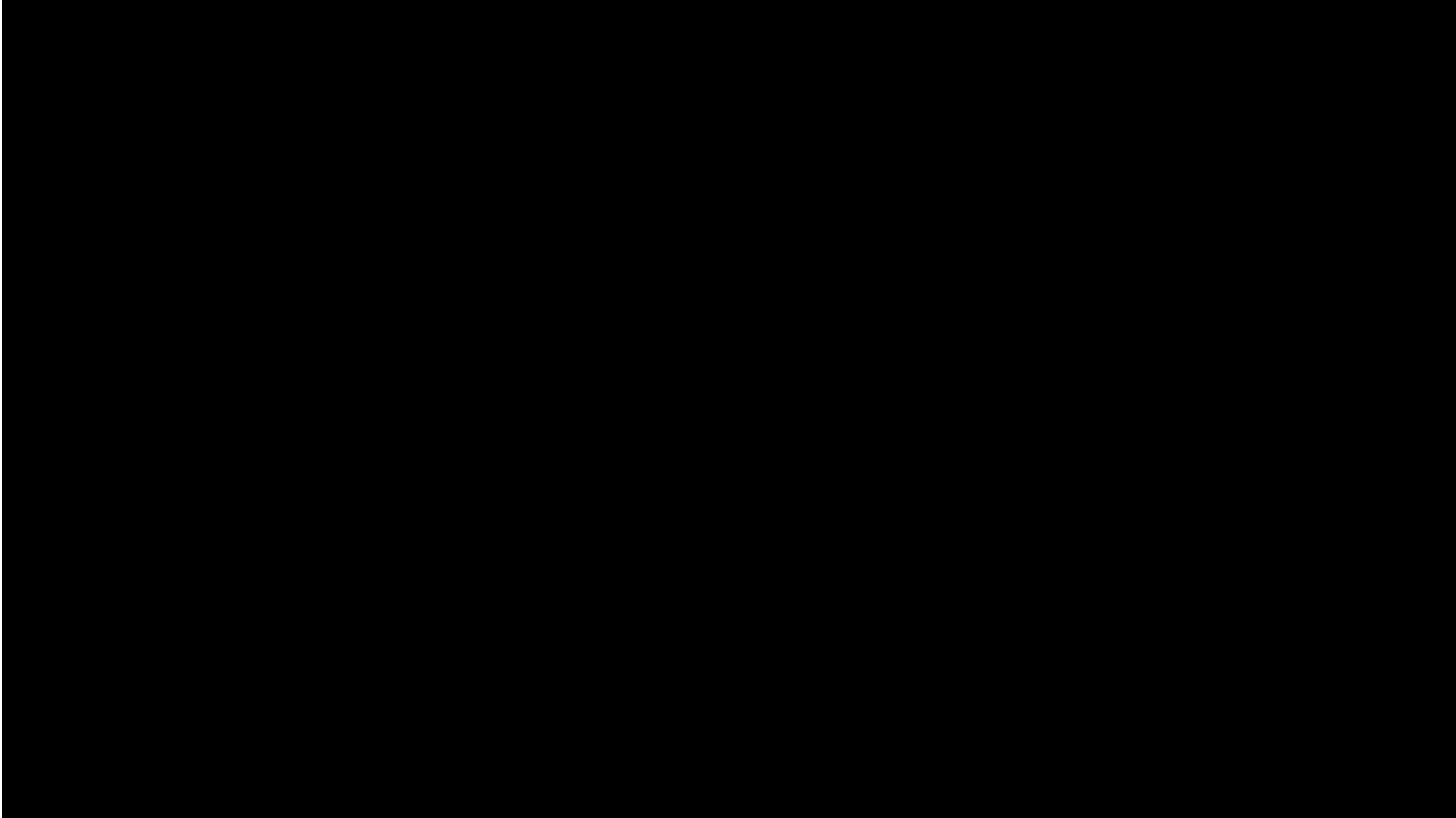
EXHIBITS AND ATTACHMENTS



EXHIBITS AND ATTACHMENTS



EXHIBITS AND ATTACHMENTS

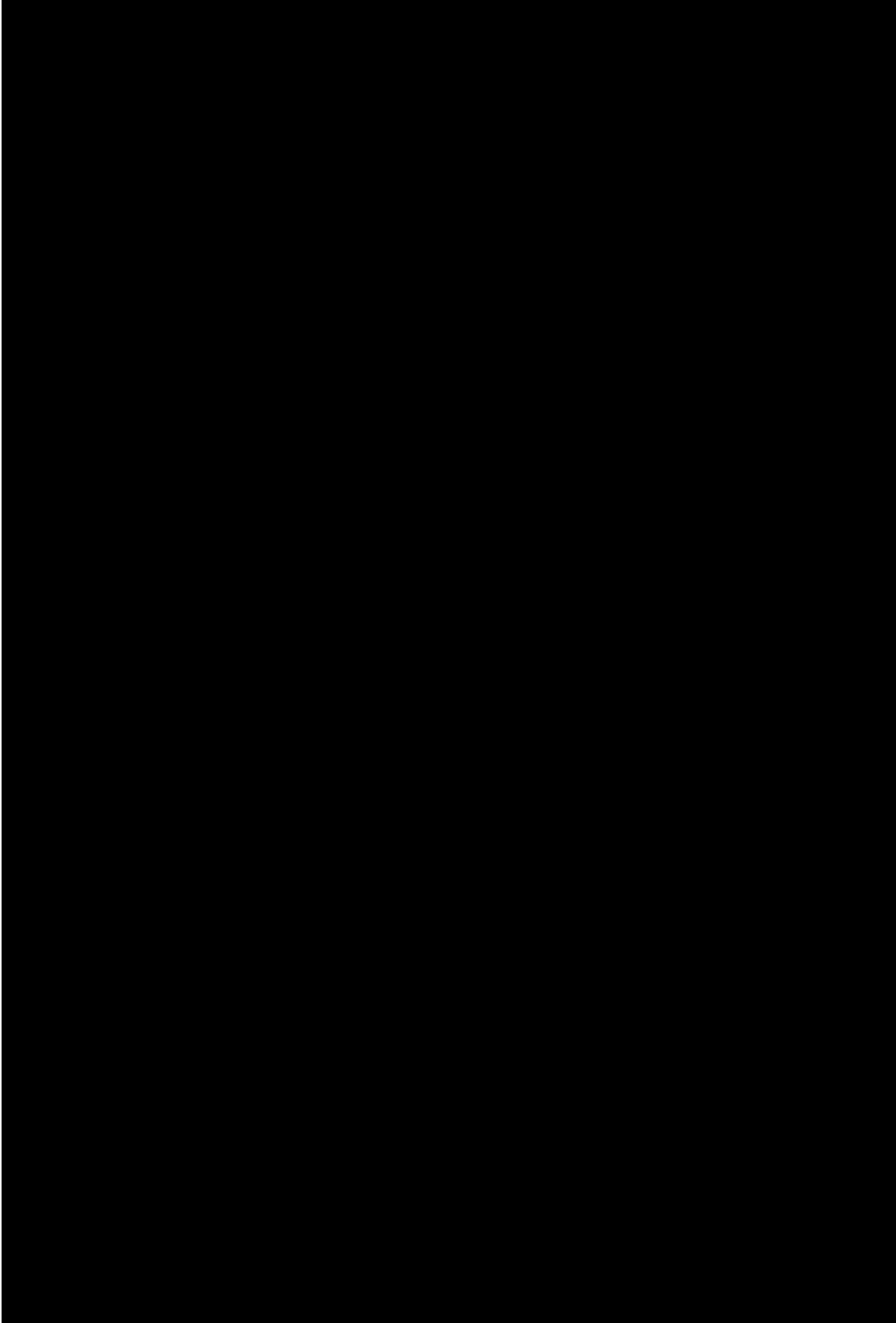


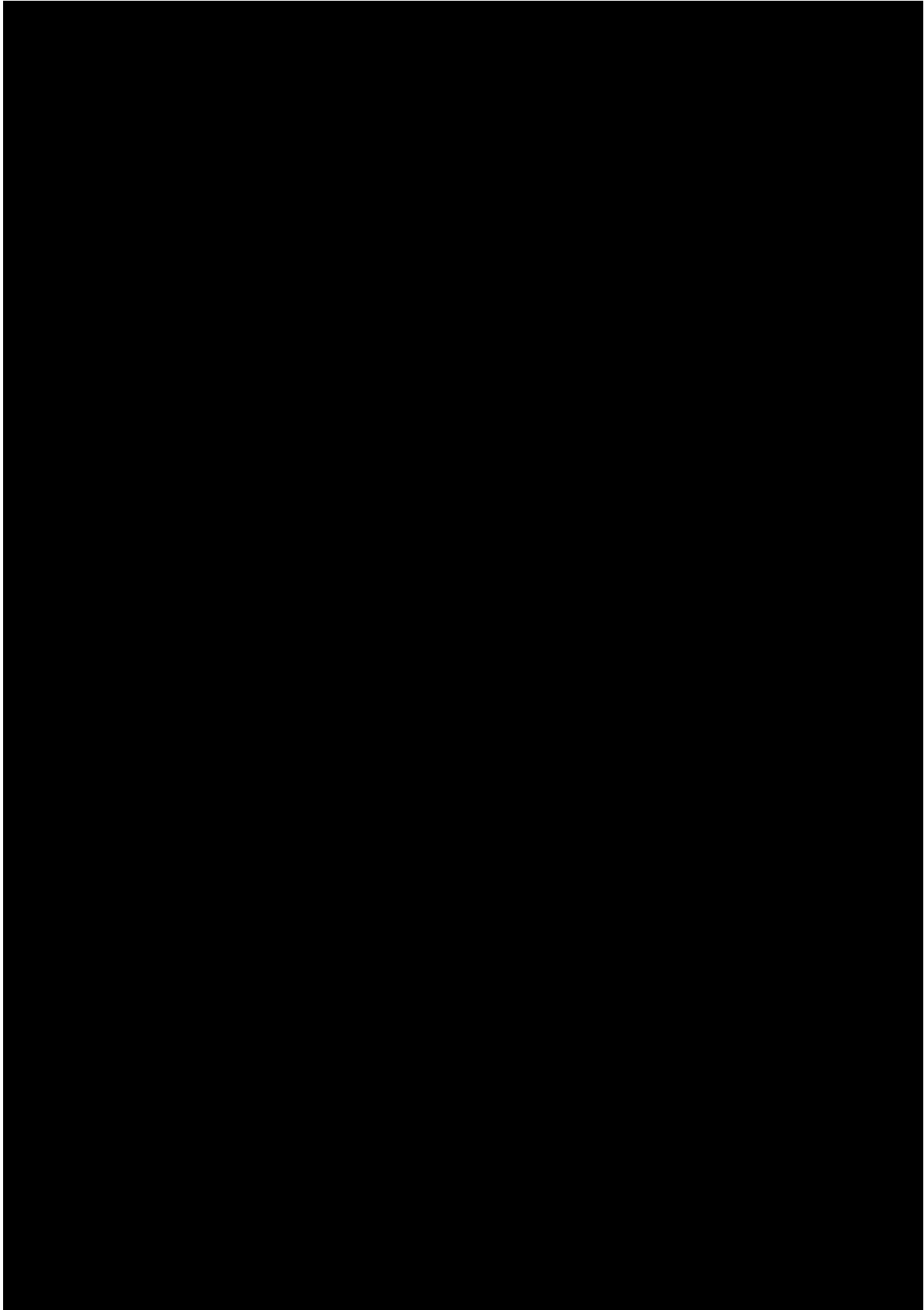
EXHIBITS AND ATTACHMENTS

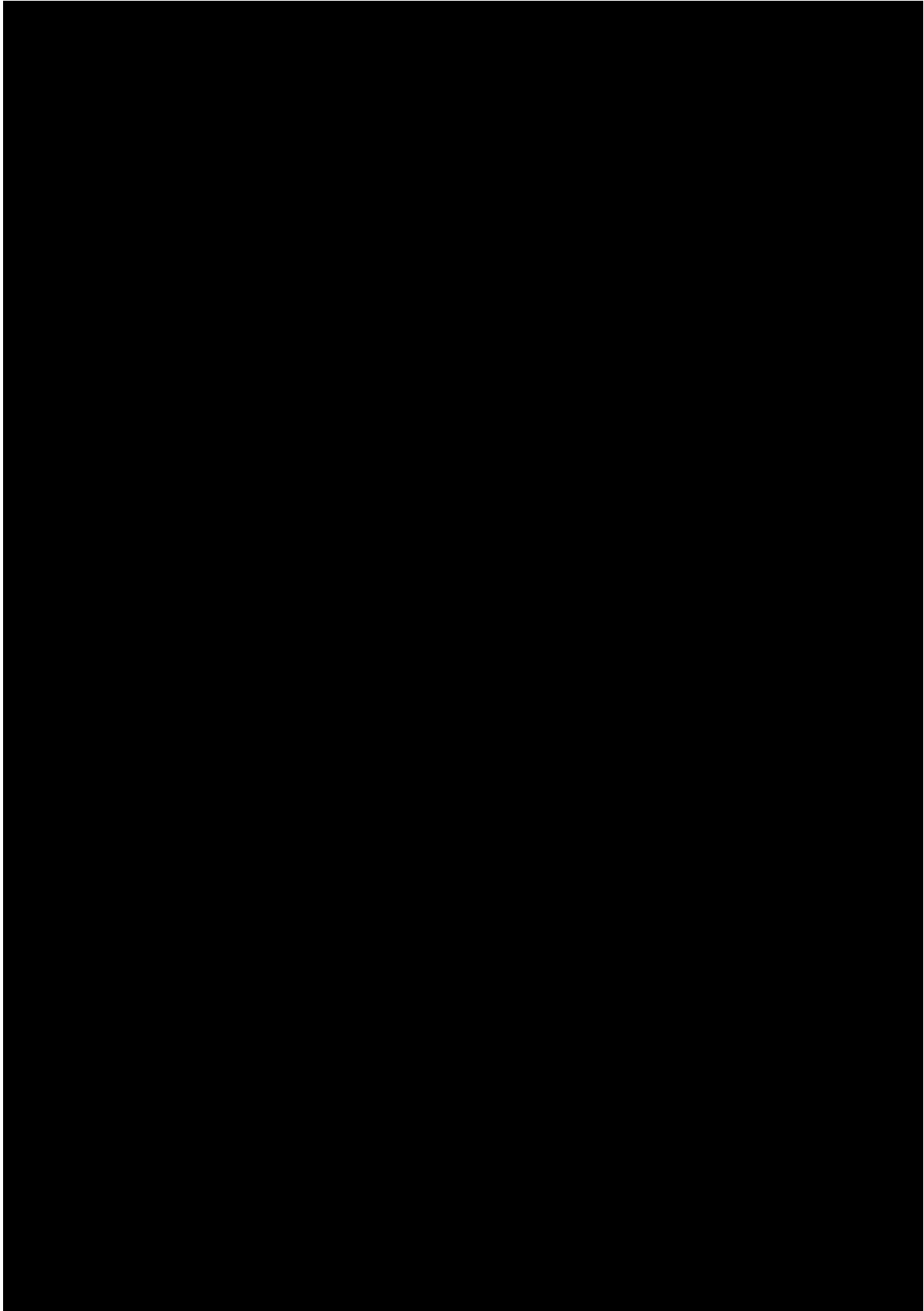
Exhibit III: Ownership Structure

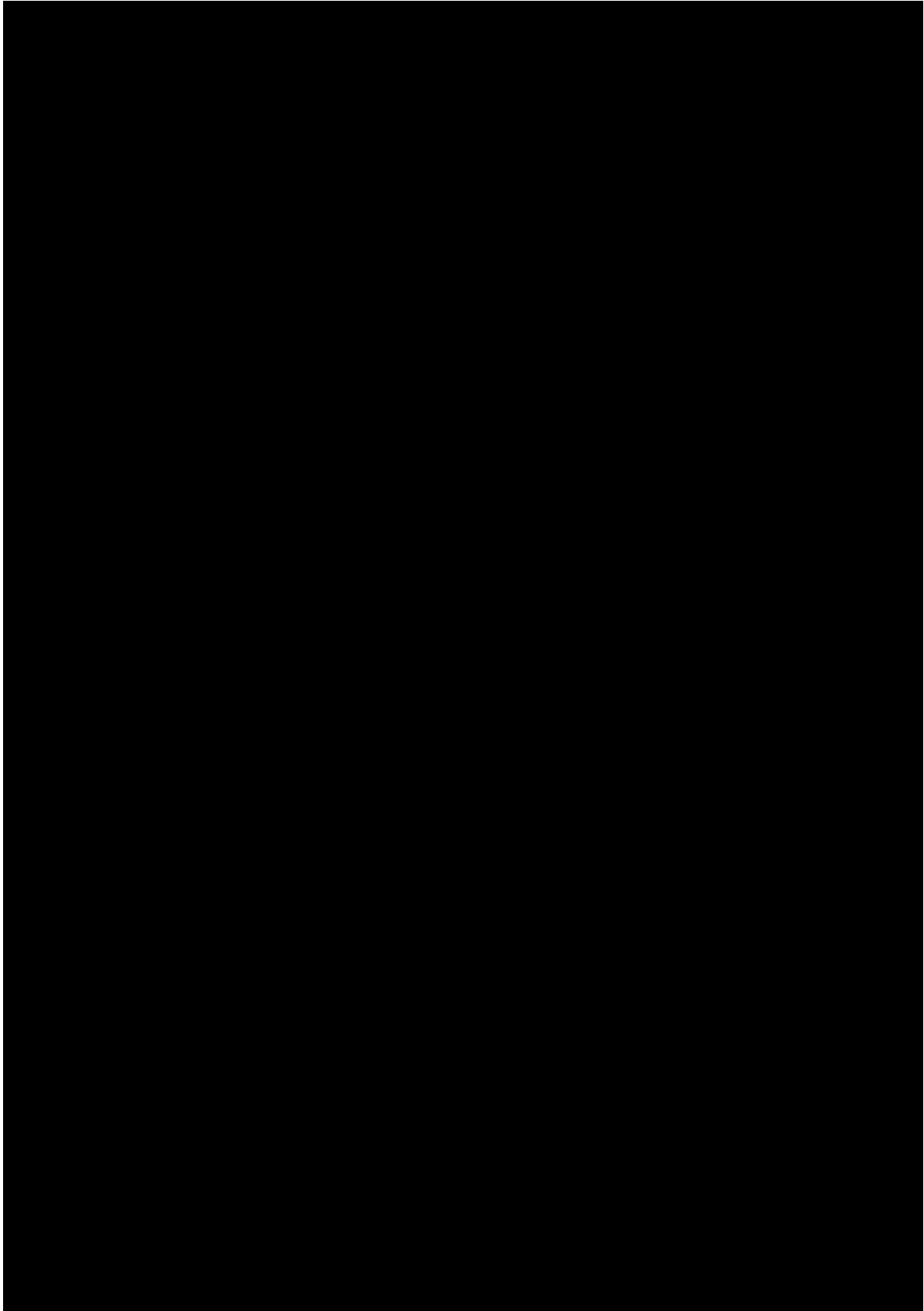
DISCLOSURE OF FINANCIAL INTEREST IN THE VENDOR - SECTION 2 - Ownership exceeding 5% or \$106,447.20			
Ownership that exceeds 5% Ownership			
NAME	Value of Ownership	Street Address	City, State, Zip address
Sentinel ESOP Trust	36.8%	2550 WARRENVILLE ROAD	DOWNERS GROVE, IL 60515
Mary Hoelzer (beneficiary of Dennis and Mary Hoelzer trust)	31.4%	1 S 920 TANGLEWOOD DRIVE	BATAVIA, IL 60510
Osborne, Brian	6.2%	13525 OAK COURT	LEMONT, IL 60439
Hill, Timothy	6.2%	574 ARLINGTON AVE	ELMHURST, IL 60126
Value of Ownership - All under 5% Ownership			
NAME	Value of Ownership	Street Address	City, State, Zip address
Elam, John	1,622,522.00	843 ALBEROSKY WAY	BATAVIA, IL 60510
Truesdale, Mike	1,280,542.00	1500 HERMITAGE DR	NEW LENOX, IL 60451
Lenartowicz, Robert	1,132,903.00	30 W 745 BRADFORD PKWY	WAYNE, IL 60184
Tedesso, Frank	1,124,617.00	4706 NORTH OCONTO AVENUE	HARWOOD HEIGHTS, IL 60706
Kunkel, Steve	1,084,694.00	13034 SPRUCE HILL CT.	LEMONT, IL 60439
Owens, Dale	643,284.00	40 W 075 EMILY DICKINSON LANE	ST. CHARLES, IL 60175
Rimkus, Jon	486,606.00	8952 LIATRIS DRIVE	FRANKFORT, IL 60423
Truesdale, Edward	486,606.00	18704 SUMMER GATE CT	MOKENA, IL 60448
Brakauskas, Sarunas	451,956.00	99 DIANA ROAD	OGDEN DUNES, IN 46368
Keblusek, Robert	266,654.00	12251 W. DONEGAL	NEW LENOX, IL 60451

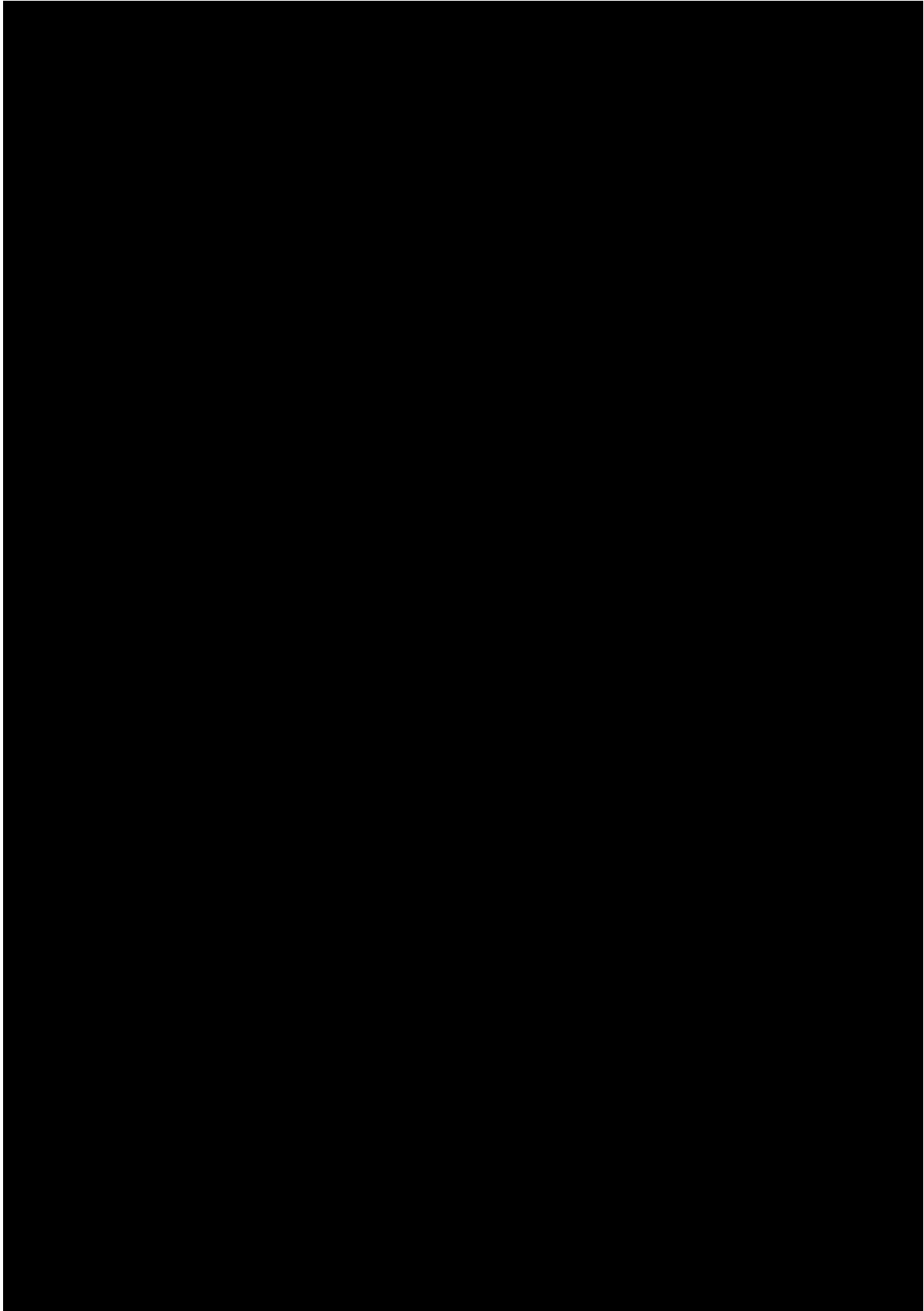
Exhibit IV: Resumes











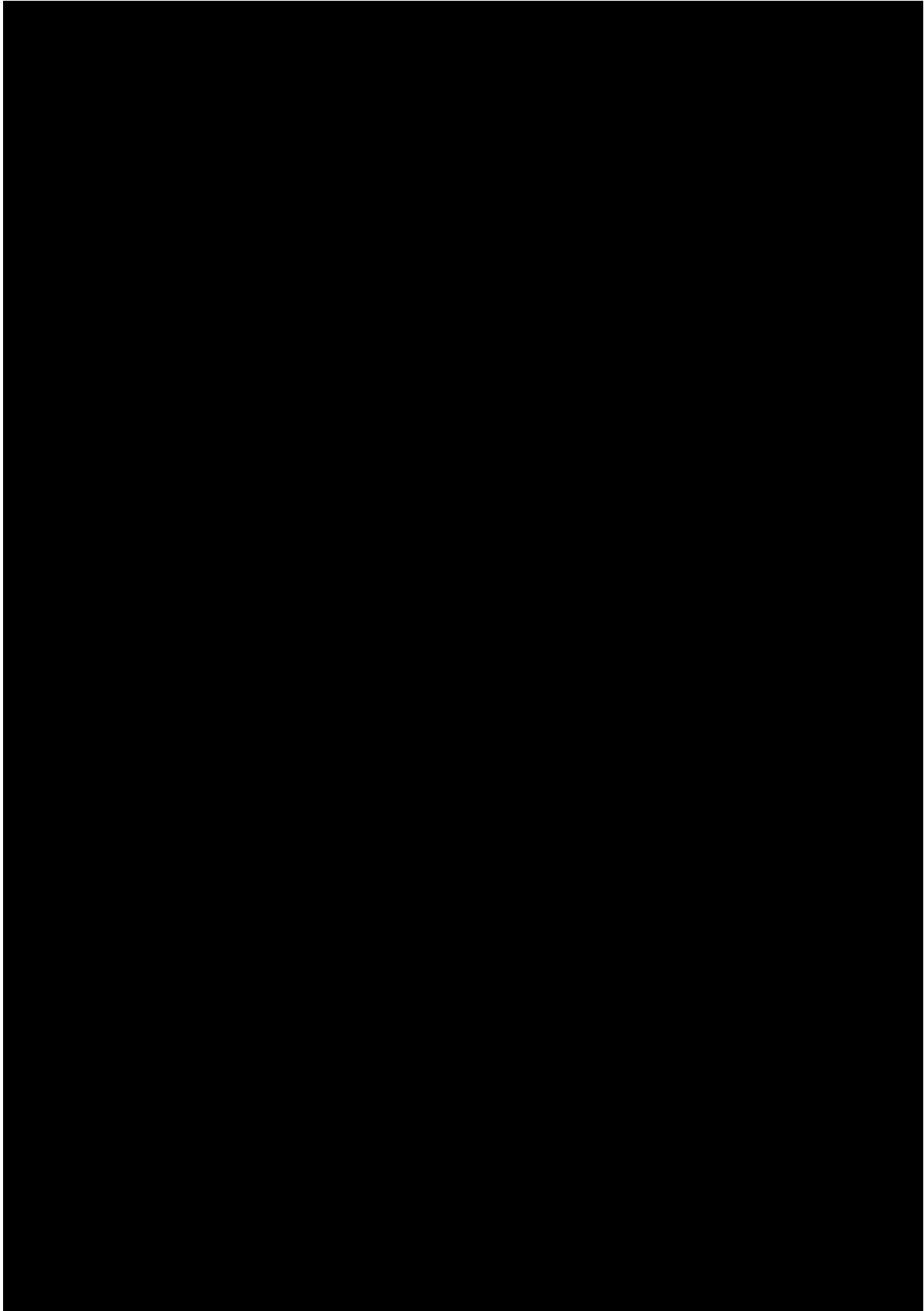


Exhibit V: Pre-Employment Screening Services

SENTINEL'S BACKGROUND INVESTIGATION

Sentinel uses an outside 3rd party company specializing in background investigation to complete the following checks:

- **Trace/SSN Verification**
The primary reason for requesting an address verification search is to confirm the current address of an applicant and to determine if there are any other names and/or addresses that should be used when performing criminal record searches. The Experian Social Search contains information from the credit bureau, which includes the various addresses, and other names associated with the applicant's social security number. The Social Search instantly matches and retrieves from Experian's database the latest consumer identification information reported on that particular social security number. This search can produce previous address and name information for people who have changed their names or moved without leaving a forwarding address.
- **Motor Vehicle Reports**
A Motor Vehicle Records (MVR) search provides the information concerning character and driving tendencies that is necessary to make a solid, well-educated hiring decision for a position that involves driving. Typically, a driving record (sometimes called an abstract or DMV Driving Report) is a history of traffic violations and license suspensions for a specific license. Information pertaining to license class, validity and issue/expiration dates may also be included.
- **Criminal History Reports**
This report is generated from state repositories and or county clerk records. Criminal records are obtained by utilizing a variety of online court services and a network of qualified public record retrievers. In addition, information is provided using a proprietary criminal record database, The National Criminal Database, which contains information from across the United States. With the National Criminal Database search, the Sex Offender Registry (includes records of 49 of 50 states and numerous Native American territories – excludes Mississippi) and the Global Vigilance Database which includes various terrorist watch lists (OFAC, FBI, Interpol, most wanted list such as BATF, DEA, FBI, ICE, and sanction lists such as FDA, OIG, GSA, FDIC, OCC, NCUA, OTS) search is conducted. The report will detail any conviction that has been made on an individual. Checks are conducted in all counties in which the applicant has lived based on 7-year address history from SS Trace, statewide checks, and Federal District Court search. Felony and misdemeanor records are reported. Misdemeanor records are obtained for the last 7 years, Felony records are obtained as far back as they occur.
- **Education Verification**
We offer degree and attendance records for GED, high school, undergraduate and graduate programs throughout the US, Canada and others parts of the world. Only verified if Degree is designated on application.
- **Employment Verification**
Previous employers are contacted to verify dates of employment, position held and

eligibility for rehire. A summary report is formatted to view applicant supplied information and employer supplied information on a one page easy to read report.

- **Sex Offender Registry – Part of Criminal History Report**
Information supplied on individuals convicted of violent sex crimes or sexual crimes involving minors. This is a check of the Sex Offender Status Registry (a government housed database) not a database compiled from various resources that are incomplete and missing information and crucial identifiers.
- **C-TPAT – Part of Criminal History Report.**
Customs-Trade Partners against Terrorism is a comprehensive check of the Bureau of Industry and Security-Denied Persons List and entities of proliferation activities, Office of Foreign Assets Control (OFAC) including SDN List and list of statutorily debarred parties.
- **Employment Verification: (going back 7 years, up to 3 employers)**
The verification of the candidate's dates of employment, job title, salary, reason for leaving, and rehire eligibility.
- **Degree/Education Verification:** Degree verification process includes the authentication of high school diplomas, GED's, and post-secondary degrees. This process confirms the candidate's dates of attendance and the type of degree earned, including the major course of study. In the event no post-secondary degree is earned, the verification process will confirm that the diploma or GED is earned.

EXHIBITS AND ATTACHMENTS

HOW SENTINEL PROTECTS ITS CLIENTS

Upon Request Sentinel will provide the following summary report to certify compliance to Sentinel’s background investigation:



BACKGROUND CHECK SEARCH SUMMARY

Report Number	Date Received	Date Complete	Employee Name
2075454	04-11-2017	04-21-2017	**BLOCKED**

SUMMARY:

Summary of Verifications Requested			
Description	Rec Date	Comp Date	Status
SOCIAL SECURITY ADDRESS REPORT: ONETRACE/ONEVALIDATION	04-11-17	04-11-17	Complete
FEDERAL DISTRICT CRIMINAL COURT SEARCH: NATIONAL NAME: **BLOCKED**	04-11-17	04-11-17	Complete/Clear
NATIONAL CRIMINAL DATABASE: NATIONAL NAME: **BLOCKED**	04-11-17	04-11-17	Complete/Clear
COUNTY CRIMINAL SEARCH (ALL COUNTIES PER NAME): COOK COUNTY, IL NAME: **BLOCKED**	04-11-17	04-12-17	Complete/Clear
COUNTY CRIMINAL SEARCH (ALL COUNTIES PER NAME): HARDIN COUNTY, KY NAME: **BLOCKED**	04-11-17	04-18-17	Complete/Clear
DRIVING RECORD CHECK: IL	04-13-17	04-13-17	Complete/Clear
PRESENT EMPLOYMENT - US SECURITY ASSOCIATES	04-11-17	04-11-17	See Report
PAST EMPLOYMENT - **BLOCKED**	04-11-17	04-21-17	Complete/Clear
PAST EMPLOYMENT - **BLOCKED**	04-11-17	04-13-17	Complete/Clear
PAST EMPLOYMENT - **BLOCKED**	04-11-17	04-14-17	Complete/Adverse
CONFIRMATION OF DEGREE - **BLOCKED**	04-11-17	04-17-17	Complete/Clear

Sentinel is very conscious to not creating a third party employment relationship. As a result, it is best practices to define parameters that would not be acceptable for the client’s environment, so that we can test our results against the client’s safety parameters. Some example parameters are as follows:

Background checks for consulting or temporary staff will, at minimum, include a complete and thorough investigation and review of any individuals presented for assignment to Client in accordance with the minimum standards set forth below.

1. The background investigation and review shall be conducted prior to an individual's placement at Client.
2. Sentinel will provide written certification to Client as depicted above that the background check and review has been conducted in accordance with these standards.
3. For workers on extended assignment or who work on additional assignments at Client Sentinel will perform the background check again if the date of the last background check is more than two years old.
4. In the event the Client requires fingerprint checks, release of detailed background investigation reports or release of personal identifying information the Sentinel Employee must provide consent to release such information to the Client. In these cases, the Client will be required to sign a confidentiality of personal information agreement to ensure the released information is to be treated and handled in a protected way by the client and only disclosed to individuals with a business need to know.
5. Minimum Standard Requirements:
 - a. Client is required by federal and state laws to take steps to avoid permitting individuals who have been convicted of a broad range of criminal offenses including, but not limited to:
 - i. Dishonesty
 - ii. Breach of trust
 - iii. Money laundering
 - b. Sentinel will investigate criminal offenses by conducting a search on all felony and misdemeanor court records for federal courts and state county courts in all jurisdictions in which an individual has resided during the last seven years, at a minimum. Individuals who have been convicted of any crime as outlined in 5a will not be permitted to be assigned to client. The only exceptions will be incidents classified as "traffic" or for a single conviction of a crime involving the following:
 - i. Driving under the influence
 - ii. Purchase liquor by minor
 - iii. Underage consumption or possession of alcohol
 - iv. Reckless driving
 - v. Underage driving
 - vi. Speeding
 - vii. Traffic signal violations
 - viii. Traffic violations misdemeanor
 - ix. Noise violation
 - x. DUI provided no driving privileges are revoked during expected contracting period
 - xi. Disorderly conduct

Exhibit VI: Sample Incident Response Agreement



APPENDIX A

Customer Name: _____

Street Address: _____

City, State, Zip: _____

The Agreement referenced below by and between Sentinel Technologies, Inc., (Contractor) with principal offices at 2550 Warrenville Road, Downers Grove, Illinois 60515, and (Customer) with principal offices at _____, is hereby appended to include the following:

Commencement Date _____ Agreement No. _____

Sentinel SecuritySelect™ Incident Response

"Incidents" are categorized as events that are influenced by elements outside of standard operating conditions and/or procedures. Such Incidents may significantly impact a Customer's systems, network, and/or business operations and may demand a response beyond the Customer's routine Incident management process.

If Customer declares an Incident and engages Sentinel's Incident Response (IR) Services, Sentinel's Incident Response Team will remain engaged until Customer expressly declares and acknowledges in writing that its normal state of operation has been restored. Sentinel's IR Team will use best efforts, pursuant to Sentinel's IR Services Rate noted herein, in addressing the Incident.

Incident Response Services

Sentinel will provide Incident Response resources to perform IR Services remotely (immediately) or on-site (within 24 hours of receipt of written request, barring travel restrictions). The Incident Response resources will work with Customer in the performance of the following services:

- Triage and investigation of the Incident to determine a response and recovery strategy.
- Provide management and coordination services and, if requested, will act as the Customer's agent throughout an active IR engagement with other vendors or suppliers. Examples include: coordination of efforts with insurers, forensics firms, consultants, public relations firms, and third-party vendors, circuit carriers, etc.
- Quarantine active threats and isolate threats and/or threat actors.
- Investigate and analyze relevant data and systems to understand the scope of the attack utilizing tools, scripts, log files, and meta-data to perform the needed forensics. Reverse engineering of malware/ransomware is not in scope.
- Work with Customer to restore systems and services to an operation state where possible.
- Monitor the environment throughout the engagement to ensure the overall health of the environment.
- Other services as requested by Customer to help respond and recover from the Incident.

Service Level Agreement (SLA)

Customer acknowledges that, due to the often complex and unpredictable nature of such Incidents, there is no guarantee that Sentinel will be able to restore Customer to its normal state of operation and agrees to hold Sentinel harmless from any damages that result from its handling of any such Incident, besides damages arising from any willful misconduct.



Incident Response Tools

Sentinel may utilize an assortment of tools during the handling of the Incident. Provisioning Fees and applicable Licensing Costs associated with the use of specific tools are included below. If the Customer purchases one of the tools from Sentinel under a separate contract, within 30 days of returning to a normal state, the associated tool-provisioning fee would be credited as a part of the sale. The Licensing costs will be billed on a monthly or annual basis as noted below until notified by the Customer, in writing, of their desire to terminate or transition one or more of the tool services at the end of the current term. Provisioning Fees and Licensing Costs are subject to change and will be reviewed with the Customer prior to deployment.

	Provisioning Fee	Licensing Fees/Cost	Notes
Umbrella	\$1,500.00	\$200 + \$3.58 Per User/Month	Minimum 100 Users
AMP	\$1,500.00	\$4.10 Per User/Month	
Cylance	\$1,500.00	\$3.64 Per User/Month	
Cylance with Optics	\$1,000.00	\$4.75 Per User/Month	
Duo (MFA)	\$3,000.00	\$200 + \$7.00 Per User/Month	
Cylance Compromise Assessment	\$22,403.15		For 1 - 2,500 Devices

Solution-Specific Terms & Assumptions

Terms & Assumptions

- Travel time will be charged in accordance with the applicable Incident Response Services Rate.
- Customer shall be charged for all out-of-pocket expenses related to the provision of Incident Response Services.
- Customer shall be charged mileage at the applicable IRS Standard Mileage Rate.
- The provision of Incident Response Services not requiring travel will carry a one (1) hour minimum charge.
- The provision of Incident Response Services requiring travel will carry a four (4) hour minimum charge.
- Unless otherwise agreed upon by the Parties, the Incident Response Rate(s) shall be fixed for one hundred eighty (180) days from the date of document execution, after which point the rates will be subject to change via through a new agreement executed between the Parties.
- Invoices will be sent to Customer on a weekly basis, which shall include all labor, materials, and expenses from the prior week's services.

Pricing Summary

The IR Rate is \$425 per hour blended rate (includes off-hours) per individual, per hour for all Incident Response Services performed. The hours incurred during the Incident will be invoiced and sent to Customer on a weekly basis, which shall include all labor, materials, and expenses from the prior week's services.

General Terms and Assumptions

- With regard to any software licenses installed by Contractor as necessary to effectuate the provision of services under this Agreement, thus not within the scope of the deliverables, Customer is hereby prohibited from duplicating said software in any form or fashion and is further restricted from using the software beyond the intended scope set forth herein. Moreover, Customer is restricted from licensing, sublicensing or transferring said software to any third party (except to a related party) without the express permission of Contractor, under which circumstance the software shall stay under the control and auspices of the Contractor. In the event Customer loses or damages the software, a copy may be provided at a nominal charge. Contractor may, at its discretion, remove said software upon the completion of its provision of services. Alternatively, at the end of this engagement or the license period, whichever occurs first, Customer is required to either destroy or return all copies of said software to Contractor, as expressly directed by Contractor.



- The manufacturer/support provider has the right to inspect any products that have either never had support coverage or have not had support coverage for an extended period to determine their eligibility for maintenance/support. Devices subject to inspection will be flagged as such and are subject to a non-refundable inspection fee, which shall be the responsibility of Customer. Sentinel will work with the manufacturer/support provider on Customer's behalf until device eligibility is determined. Devices that do not pass the inspection will be ineligible for support.
- For products purchased pursuant to this agreement, Contractor agrees to provide storage at no additional charge for up to 90 days. If the storage period exceeds 90 days, Customer agrees to the following: a.) Customer will be responsible to pay a fee of 2% per month for storage of purchased products from that point forward, b.) Customer will be invoiced and will be responsible to pay the unpaid balance for any products purchased from Contractor that have not been paid in full and, c.) Ownership will transfer from Contractor to Customer.
- For all products purchased, it is assumed that prior to order execution with Contractor, Customer has reviewed, understood, and agreed to each manufacturer's respective terms and conditions governing the purchase of products, including, but not limited to, applicable warranties, order cancellation, and return policies. In the event of a return request, Sentinel may assist Customer by facilitating the request between Customer and the manufacturer. In addition, product return requests will be subject to Sentinel's own return policies, which may include restocking fees and/or shipping and handling costs.
- Under no circumstances will Customer have the right to withhold payment to Sentinel due to an alleged breach of any express or implied warranties with regard to the products purchased herein. Any such claim shall be handled directly between the manufacturer and Customer. If Contractor receives any financial relief or incentives intended for Customer as a result of a settlement between Customer and the manufacturer, Contractor agrees to pass through the incentives or financial relief to Customer.

Payment Terms

All Invoices: Net 30

This quote is valid until / / 20 .

CUSTOMER:

CONTRACTOR:

Sentinel Technologies, Inc.

Signature: _____

Signature: _____

Printed Name: _____

Printed Name: _____

Title: _____

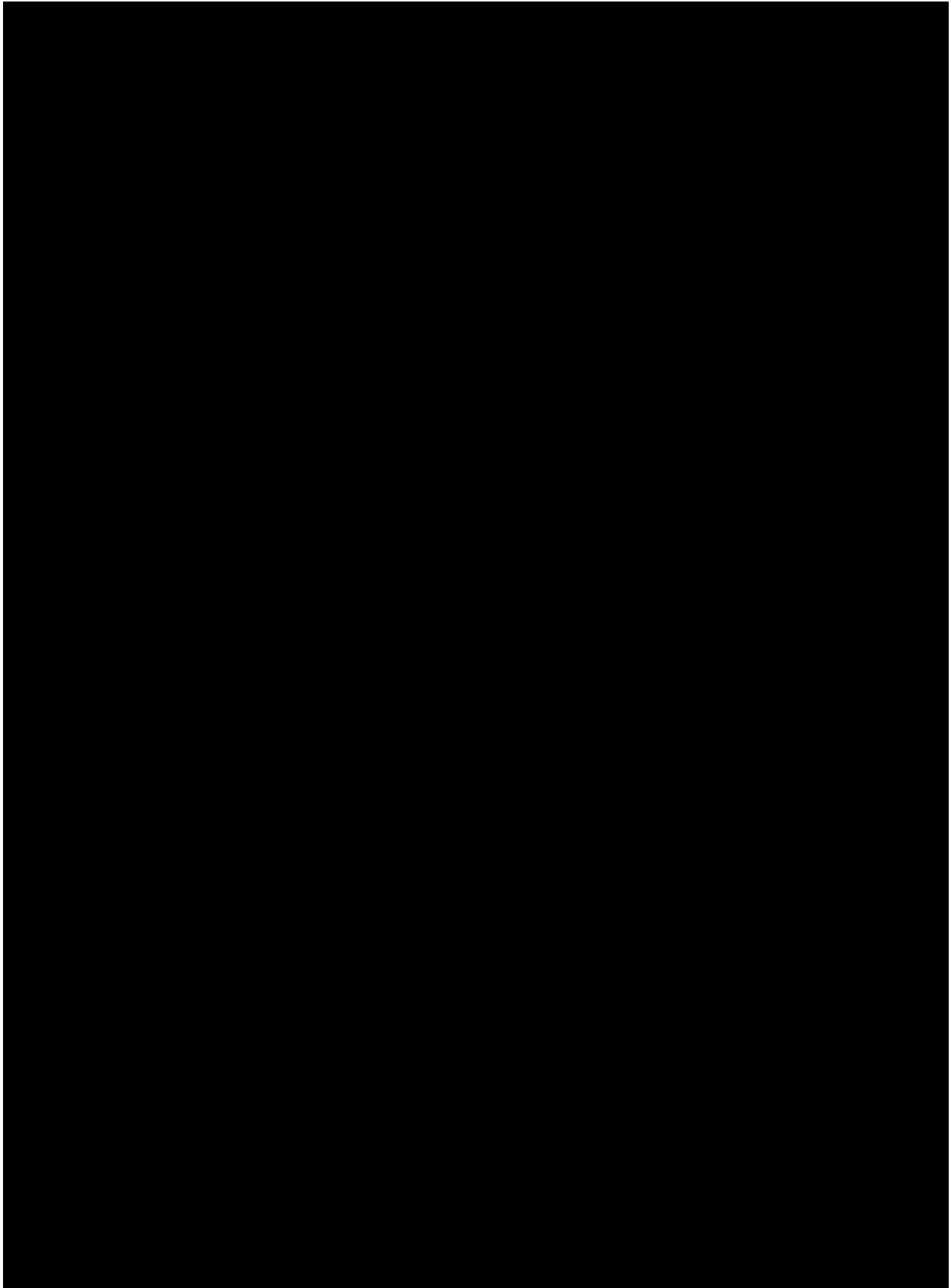
Title: _____

Date: _____

Date: _____

P.O. #: _____

Exhibit VII: Sample Certificate of Insurance



EXHIBITS AND ATTACHMENTS

Exhibit VIII: Inventory

Product Type	Device Name	Machine Type	Model	Product Quantity
Compute System Controller	HX - A	Cisco	HX-FI-6454	1
Compute System Controller	HX-B	Cisco	HX-FI-6454	1
Firewall Security Device	CTPF-FMC.ctpf.org.(none)	net-snmp - Linux	VIRTUAL	1
Firewall Security Device	CTPF-FTD-1	Firepower 2120	ASA5516-FPWR-K9	1
Firewall Security Device	CTPF-FTD-1	Firepower 2120	FPR2120-NGFW-K9	1
Hypervisor	vcenter01.ctpf.org	Unknown	VIRTUAL	1
LAN Switch	CTPF-AV-1.ctpf.org	Cisco C9200L	C9200L-48P-4X-A	1
LAN Switch	CTPF-CORE-1.ctpf.org	Catalyst 9500-48Y4C	C9500-48Y4V-A	1
LAN Switch	CTPF-IDF-15-1.ctpf.org	Cisco C9200L	C9200L-49P-4X-A	1
LAN Switch	CTPF-MDF-1.ctpf.org	Cisco C9200L	C9200L-48P-4X-A	8
Linux Server	ctpf.org website	Unknown	VIRTUAL	1
Linux Server	ec2-3-20-252-54.us-east-2.compute.amazonaws.com	Unknown	WEBSITE	1
Linux Server	mariadb-1.cctiqoftp17.us-east-2.rds.amazonaws.com	Unknown	WEBSITE	1
Linux Server	mssfsprod.ctpf.org	Unknown	SERVER	1
NetFlow Traffic Analysis	05016-CSR-1.cloud.sentinel.com	Cisco	CSR1000V	1
NetFlow Traffic Analysis	05016-CSR-2.cloud.sentinel.com	Cisco	CSR1000V	1
NOC Monitoring + Alerting - Network/UPS	RA32-MDF	AVTECH	Avtech RA32e	1
WAN Routers-Voice Gateway	CTPF-COAGENT-4451.ctpf.org	Cisco ISR4451	ISR4451-X-SEC/K9	1
WAN Routers-Voice Gateway	CTPF-ZAYO-4451.ctpf.org	Cisco ISR4451	ISR4451-X-SEC/K9	1
Wireless Access Point (WLC)	CHIWC01-VIP	Cisco 3504 Wireless LAN Controller	AIR-CT3504-K9	14
Wireless Controller	CHIWC01-VIP	Cisco 3504 Wireless LAN Controller	AIR-CT3504-K9	1

For visibility purposes, Sentinel has attached a copy of your current inventory that is being monitored and managed as this inventory differs from the inventory included within the RFP.