Please provide the following:

Number	Item
1	Current SOC 2 Type 2, ISO 27001, or other third-party attestation report. If a third-party attestation report is unavailable, identify which controls are used at your company on the **Cybersecurity Controls tab**.
2	Current penetration test results and proof of remediation for critical and high findings
3	Current vulnerability test results and proof of remediation for critical and high findings
4	Evidence of cybersecurity insurance

Identify

Control ID	Control	Yes	No
AM-1	Physical devices and systems within the organization are inventoried.		
AM-2	Software platforms and applications within the organization are inventoried.		
AM-3	Organizational communication and data flows are mapped.		
AM-4	External information systems are catalogued.		
AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.		
BE-1	The organization's role in the supply chain is identified and communicated.		
BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated		
BE-3	Dependencies and critical functions for the delivery of critical services are established.		
BE-4	Resilience requirements to support the delivery of critical services are established for all operating states (e.g., under duress or attack, during recovery, normal operations.)		
GV-4	Governance and risk management processes address cybersecurity risks.		
RA-1	Asset vulnerabilities are identified and documented.		
RA-2	Cyber threat intelligence is received from informationsharing forums and sources.		
RA-3	Threats, both internal and external, are identified and documented.		
RA-4	Potential business impacts and likelihoods are identified.		
RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to assess risk.		
RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders.		
RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.		
SC-2	Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process		
	Protect		
AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.		
AC-2	Physical access to assets is managed and protected.		
AC-3	Remote access is managed.		
AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.		
AC-5	Network integrity is protected (e.g., network segregation, network segmentation).		
AC-6	Identities are proofed and bound to credentials and asserted in interactions.		
AC-7	Users, devices, and other assets are authenticated (e.g., singlefactor, multi- factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).		
AT-2	Privileged users understand their roles and responsibilities.		
AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.		
DS-1	Data at rest is protected.		
DS-2	Data in transit is protected.		
DS-3	Assets are formally managed throughout removal, transfers, and disposition.		
DS-4	Adequate capacity to ensure availability is maintained.		
DS-5	Protections against data leaks are implemented.		
DS-6	Integrity-checking mechanisms are used to verify software, firmware, and information integrity		
DS-8	Integrity checking mechanisms are used to verify hardware integrity.		

Note: These controls are based on NIST IR 8323r1

IP-1	A baseline configuration of information technology / industrial control systems are created and maintained that incorporates security principles (e.g. concept of least functionality) is created and maintained.		
IP-2	A System Development Life Cycle to manage systems is implemented.		
IP-3	Configuration change control processes are in place.		
IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.		
IP-10	Response and recovery plans are tested.		
MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools		
MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access		
PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.		
PT-2	Removable media is protected, and its use restricted according to policy.		
PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.		
PT-4	Communications and control networks are protected.		
PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.		

Detect

Control ID	Control	Yes	No
AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.		
AE-2	Detected events are analyzed to understand attack targets and methods.		
AE-3	Event data are collected and correlated from multiple sources and sensors.		
AE-4	Impact of events is determined.		
AE-5	Incident alert thresholds are established.		
CM-1	The network is monitored to detect potential cybersecurity events.		
CM-2	The physical environment is monitored to detect potential cybersecurity events		
CM-3	Personnel activity is monitored to detect potential cybersecurity events.		
CM-4	Malicious code is detected.		
CM-5	Unauthorized mobile code is detected.		
CM-6	External service provider activity is monitored to detect potential cybersecurity events.		
CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.		
CM-8	Vulnerability scans are performed.		
DP-1	Roles and responsibilities for detection are well- defined to ensure accountability.		
DP-3	Detection processes are tested.		
DP-4	Event detection information is communicated.		
DP-5	Detection processes are continuously improved.		

Response

Control ID	Control	Yes	No
RP-1	Response plan is executed during or after an incident.		
CO-1	Personnel know their roles and order of operations when a response is needed.		
CO-2	Incidents are reported consistent with established criteria.		
CO-3	Information is shared consistent with response plans.		

CO-4	Coordination with stakeholders occurs consistent with response plans.		
AN-1	Notifications from detection systems are investigated.		
AN-2	The impact of the incident is understood.		
AN-3	Forensics are performed.		
AN-4	Incidents are categorized consistent with response plans.		
AN-5	Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).		
MI-1	Incidents are contained.		
MI-2	Incidents are mitigated.		
MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks.		
IM-1	Response plans incorporate lessons learned.		
IM-2	Response strategies are updated.		

Recovery

Control ID	Control	Yes	No
RP-1	Recovery plan is executed during or after a cybersecurity incident		
IM-1	Recovery plans incorporate lessons learned.		
IM-2	Recovery strategies are updated.		
CO-1	Public relations are managed.		
CO-2	Reputation is repaired after an incident.		
CO-3	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.		