Cybersecurity Document Request List

Below is a list of items necessary to complete the Cybersecurity review. All items should be available at the start of the examination. Please number the items to correspond with the numbering system below and provide electronic versions of documents or reports when possible. Please also provide a listing of any items that are not applicable or available and indicate why.

1. **Cyber Risk Management & Oversight**

    A. Organization chart
    B. Cybersecurity related policies and procedures
    C. Board/IT Committee minutes
    D. Strategic plans
    E. Employee incentive plans
    F. Cybersecurity job descriptions
    G. Cybersecurity personnel qualifications
    H. Risk assessments
    I. IT Audit schedule
    J. Engagement letters
    K. IT Audit reports and correspondence (includes financial audit if there were IT or Cybersecurity scope areas)
    L. Audit exception tracking (with emphasis on IT/Cybersecurity audits)
    M. Risk management reports
    N. Documentation evidencing employees have completed cybersecurity training and awareness training
    O. Cybersecurity training policies and procedures
    P. Cybersecurity training and awareness materials

2. **Cybersecurity Controls**

    A. List of physical access controls (such as key cards, biometric controls, video cameras)
    B. Baseline security configuration standards
    C. Software Development Life Cycle (SDLC)
    D. Vulnerability/patch management policies and procedures
    E. Patch management reports
    F. Penetration test results/reports
    G. Vulnerability assessments

3. **External Dependency Management**

    A. List of third parties and subcontractors
    B. Contracts governing all third-party relationships
    C. Inventory of all third-party connections, including connections to:
        i. Customers;
        ii. Third-party service providers;

iii. Business partners, and;
iv. Other Internet connections (e.g., web server, remote maintenance, etc.)

D. Network topology/diagram
E. Independent reports on the service provider's security controls
F. Remote access logs
G. Third-party employee access reviews
H. Vendor Management policies and procedures

4. Threat Intelligence and Collaboration

A. List of threat intelligence resources (e.g. industry groups, consortiums, threat and vulnerability reporting services)
B. Management reports on cyber intelligence

5. Cyber Resilience

A. Cybersecurity event log and reports on cyber incidents
B. Business Impact Analysis
C. Business/Corporate Continuity Plan
D. Results of resilience testing
E. Resilience testing reports
F. Cyber incident response plans
G. Crisis management plans