Attachment 1: Cybersecurity Program Checklist

[This Checklist is adapted from Sharon D. Nelson, David G. Ries and John W. Simek, *Locked Down: Practical Information Security for Lawyers, Second Edition* (American Bar Association 2016).]

A comprehensive cybersecurity program should include the following elements. While checklists are helpful for cybersecurity programs, it important to use them appropriately. Security is not a "check the box" or "set it and forget it" process. It is important to devote continuing attention to security and to periodically review and update cybersecurity programs.

- □ **Assignment of responsibility for security,**
- □ **Managing and minimizing data,**
- □ **An inventory of information assets and data,**
- □ **A risk assessment,**
- □ **Appropriate administrative, technical and physical safeguards to address identified risks,**
- □ **Managing new hires, current employees and departing employees**
- □ **Training,**
- □ **An incident response plan,**
- □ **A backup and disaster recovery program,**
- □ **Managing third-party security risks, and**
- □ **Periodic review and updating.**

Provided by:
David. G. Ries
Clark Hill PLC
Pittsburgh, PA
dries@clark hill.com
412.394.7787