Working with Vendors to Enhance Cybersecurity
Agenda

Why Cybersecurity supplement – CIA Triad
Contract Lifecycle
Security Supplement
Why should you care about vendors?

• Stolen credentials
• Ransomware
• Backdoor
• Lack of data encryption

It’s not a question of if, but when...

• Target
• Solarwinds
• Kaseya
CIA Triad

Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity – guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.

Availability – ensuring timely and reliable access to and use of information.
Data & Risk

<table>
<thead>
<tr>
<th>Location</th>
<th>Type of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud</td>
<td>Election &amp; Business Records</td>
</tr>
<tr>
<td></td>
<td>Privacy Information</td>
</tr>
<tr>
<td>On-Prem</td>
<td>Financial Transactions</td>
</tr>
<tr>
<td></td>
<td>Access Vendor Info only</td>
</tr>
</tbody>
</table>
Contract Lifecycle: Cybersecurity

Identify need

Setup
Define expectations
Mitigate risk

Monitor
Monitor performance
- Daily
- Monthly/Semi annual
- Annual

Define Scope

Contract Terms. Including:
- Legal terms
- Deliverables
- SLAs
- Cybersecurity terms

Frank LaRose
Ohio Secretary of State
Security Supplement - People

• Require criminal background checks
• Access control – least privilege
• Staff training
Security Supplement - Processes

- Vulnerability management and application security
- Incident response policy and process
- Engagement expectations during incident response activity
- Data handling expectations
- Engagement with federal partners
- Supply chain risks
- Regulatory compliance
Security Supplement - Technology

• Network/wireless controls
• Email standards (DMARC/SPF)
• Detection and prevention tools
• Penetration and control testing
• Password requirements/MFA
• Secure baseline images
• Remote access controls
• Data encryption