Contract Considerations for Cyber Risk Management

Marc Hiller, Supervising Attorney, OGS
Joel Lombardi, Associate Attorney, Bureau of House Counsel, ITS
Carey Merrill, Special Counsel for Ethics, Risk & Compliance, ITS

June 8, 2017
Overview

• What contracts should be considered for cyber risk?
• What is vendor due diligence in the context of cyber risk?
• What terms and considerations may be necessary?*
• What provisions are included in existing State resources?*
• Where is there additional guidance?

*Samples are provided for discussion purposes only and are not intended as legal advice
What contracts should be considered?

- Physical Access to Information Systems
- Virtual Access to Information Systems
- Any Access to Software Code
- Any Access to Intellectual Property
- Purchased Software/Hardware
What is vendor due diligence in the context of cyber risk?

- Vendor reputation
- Certifications
- Background checks, qualifications and training of personnel
- Assessment of security practices and protocols
- Assessment of incident response, business continuity, disaster recovery plans
- Assessment of controls
- Regulatory compliance review
- Audit results
- Compliance and risk assessment results
What terms and considerations may be necessary?

Comprehensive definitions
- Examples: breach, confidential information, cyber incident, data, data breach expenses, personal information, vulnerability

Data Access, Use, and Disclosure
- Any data provided shall be used solely for the purposes set forth in the contract.
- Enter into nondisclosure agreements as required for the access to systems, information, or data.
- No data transmitted, exchanged, or otherwise provided to others, except as expressly agreed to in writing by the state agency.
- Designated devices.
- Data encryption requirements.

Handling of Data
- Physical Data Transport, Data Transmission

Security Policies & Procedures
- Preserve the confidentiality, integrity and accessibility of State data with administrative, technical and physical measures that conform to federal, State and Agency mandates, and generally recognized industry standards and practices, to include the National Institute of Standards and Technology (NIST) 800-53 guidelines for implementing system security and privacy controls. Accordingly, Contractor must comply with State security policies and procedures, including but not limited to…

Security Practices
- **Contractor Network Security Measures:** The contractor agrees to maintain network security that, at a minimum, includes network firewall provisioning, intrusion detection, and at least two annual third-party vulnerability assessments, which shall be available for review and/or audit upon state agency request.
- **Contractor Personnel Security Measures:** The contractor, its agents, officers, employees, partners and subcontractors shall comply with all security procedures of the State, to include security clearances, national criminal background checks, and fingerprinting (including contractor payment of the costs associated therewith).

Service Level Agreement Requirements

Samples are provided for discussion purposes only and are not intended as legal advice.
Information Security Measures

- Contractor Information Security Measures: The contractor must have written policies, procedures, practices, and controls that protect information from unauthorized disclosure, use, access, loss, alteration or destruction, and must agree that it will protect information in accordance with commercially recognized industry standards and practices. Furthermore, the contractor shall use appropriate administrative, technical, and physical security measures to preserve the privacy, confidentiality, integrity, and availability of confidential information. The state agency shall have the right to review the policies, procedures, practices, and controls related to the protection of state agency data and information.

Compliance with State & Federal Laws, Rules, Regulations & Policies

- Contractor must also comply with State and Federal laws, rules, regulations, and policies, as well as all State and Authorized User policies regarding compliance with various confidentiality and privacy laws, rules and regulations, including but not limited to NYS Technology Law, Health Insurance Portability and Accountability Act (HIPAA); the Health Information Technology for Economic and Clinical Health Act (HITECH); IRS Publication 1075; Code of Federal Regulations, Title 42: Public Health, Part 2 – Confidentiality of Alcohol and Drug Abuse Patient Records; Family Educational Rights and Privacy Act (FERPA); the federal Driver’s Privacy Protection Act of 1994 (DPPA); the Criminal Justice Information Services (CJIS) Security Policy.

Incident notification/response/cooperation

- In the event of a security incident, as defined by ISBNA, Contractor shall notify ITS within 4 hours of becoming aware of the breach and commence an investigation in cooperation with ITS to determine the scope of the breach. Contractor shall also take immediate and necessary steps needed to restore the information security system to prevent further breaches, as well as immediately preserve any potential forensic evidence relating to the incident. Except as otherwise instructed by ITS, the Contractor shall, to the fullest extent possible, first consult with and receive authorization from ITS prior to notifying any individuals, the State Consumer Protection Board, or the Office of the Attorney General (OAG) or any consumer reporting agencies of a breach of the security of the System or concerning any determination to delay notification due to law enforcement investigations. The Contractor shall fully cooperate with the State in investigating any breach, security incident or vulnerability, to include cooperation with activities necessary for the State to determine the need for notification and/or to provide the notification(s) required.

Samples are provided for discussion purposes only and are not intended as legal advice.
Responsibility for Costs Associated with a Breach

• The contractor shall be liable for the costs associated with a breach if caused by the contractor’s negligent or willful acts or omissions, or the acts or omissions of the contractor’s agents, officers, employees, partners or subcontractors.

Right to Inspect/Audit Security Practices

• The State has the right to review Contractor’s procedures, practices and controls related to the protection of Agency data and information assets. Upon request, Contractor will make available for review policies, procedures, practices and documentation related to the protection of State data and information assets, including but not limited to related to information security governance, network security, risk and compliance management policies and procedures, personnel security background screening/checks and vetting procedures, secure systems/software development protocols, change/release management, testing, quality assurance, vulnerability management, secure disposal/sanitization and documentation. Contractor may be asked to provide a recent independent audit report on security controls prior to formal awarding of any contract resulting from this RFP or at any time during the Contract term. The State and any regulatory authority having jurisdiction over the State or Authorized Users shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations used in the performance of any work under the resulting Contract. On the basis of such inspection, specific measures may be required in cases where the Contractor is found to be noncompliant with Contract safeguards.

Risk Assessment

• The Contractor shall provide a certified copy of the Security Risk Assessment to the State within 30 days of completion (assuming State exercises the option to conduct such an assessment). Issues identified in the Risk Assessment should be addressed with a plan for resolution, and resolved within 90 days of the Risk Assessment.

Insurance requirements

• **Cyber Liability Insurance:** The contractor shall provide cyber liability insurance which must include, at a minimum [coverage for privacy liability, network security liability, media and intellectual property liability, professional liability, notification and credit monitoring expenses, crisis management costs, computer forensics services, privacy regulatory defense and penalties, third party electronic theft and computer fraud, and network interruption and recovery].

Samples are provided for discussion purposes only and are not intended as legal advice.
What terms and considerations may be necessary?

Other items:

- Preservation and Disposal of Data
- Termination and Transition Requirements
- Contingency Plans
- Subcontracting
- Suitability Determinations, Security Clearances & Background Checks
- Training & Qualifications

Samples are provided for discussion purposes only and are not intended as legal advice.
What provisions are included in existing State resources?

Appendix A
Standard Clauses for New York State Contracts

22. COMPLIANCE WITH NEW YORK STATE INFORMATION SECURITY BREACH AND NOTIFICATION ACT. Contractor shall comply with the provisions of the New York State Information Security Breach and Notification Act (General Business Law Section 899-aa; State Technology Law Section 208).

Samples are provided for discussion purposes only and are not intended as legal advice.
New York State Information Security Breach and Notification Act

General Business Law Section 899-aa

“Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.”

“Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.”

State Technology Law Section 208

“Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.”
What provisions are included in existing State resources?

**IT Procurements: OGS Umbrella Contract**

In 2015 OGS established the Information Technology Umbrella Contract – Manufacturer Based (Statewide) (“Umbrella Contract”) that includes Cloud services.

The Umbrella Contract covers the following four lots:

- Lot 1 – Software
- Lot 2 – Hardware
- Lot 3 – Cloud
- Lot 4 – Implementation Services

[https://ogs.ny.gov/purchase/snt/awardnotes/7360022802can.HTM](https://ogs.ny.gov/purchase/snt/awardnotes/7360022802can.HTM)

Samples are provided for discussion purposes only and are not intended as legal advice
This is how some of the Cloud services issues are dealt with in the Umbrella Contract:

1. Transportation of Data
   - §3.7.1, Transferring of Data, General; and
   - §3.8, Encryption

2. Data Location
   - §3.5.4, Data Location and Related Restrictions

3. Security of Data
   - §3.8, Encryption;
   - §3.10, Security Processes; and
   - §3.14, Access to Security Logs and Reports

4. Contractor Access to Data
   - §3.5.3, Contractor Access to Data; and
   - §3.16, Personnel

5. Ownership and Access to Data
   - §3.5.1, Data Ownership;
   - §3.5.2, Authorized User Access to Data; and
   - §3.13, Secure Data Disposal

6. Transition of Data at End of Contract
   - §3.7, Transferring of Data; and
   - §3.17, Business Continuity/Disaster Recovery (BC/DR) Operations

7. Insurance requirements
   - §2.9 and Appendix J, Contractor’s Insurance Requirements;
   - Appendix B, §63B, Limitation of Liability for Lot 3; Contractor and Reseller Information (designates Cloud offerings – low, medium, and high risk)

Samples are provided for discussion purposes only and are not intended as legal advice
This is how some of the Cloud services issues are dealt with in the Umbrella Contract:

8. Support Services
   – §3.5.5, Support Services;
   – §3.5.6, Infrastructure Support Services

9. Data center locations; diversity and redundancy
   – §3.5.4, Data Location and Related Restrictions; and
   – 3.17, Business Continuity/Disaster Recovery (BC/DR) Operations

10. Changes in service offerings (dynamic and one-to-many model)(private/public cloud)
    – §3.20, Modification to Cloud Service Delivery Type and Description within an Authorized User Agreement

Samples are provided for discussion purposes only and are not intended as legal advice.
APPENDIX F - PRIMARY SECURITY AND PRIVACY MANDATES

New York State considers the protection of sensitive and confidential information and business systems to be of the upmost importance. The information collected and maintained by state and local government agencies is protected by a myriad of Federal and State laws and regulations. **Access to and use of sensitive and confidential information is limited to authorized government employees and legally designated agents, for authorized purposes only.**

The following chart reflects several significant federal and state laws, rules and regulations, policies, standards and guidelines that providers doing business with the State must be aware of. Links to further guidance are included. **The list is intentionally US-centric, and is not intended to be all-inclusive.** Further, since laws, regulations, requirements and industry guidelines change, consulting definitive sources to assure a clear understanding of compliance requirements is critical. Many agencies have additional program compliance requirements that must be considered in addressing compliance. (e.g., DMV Privacy Act, Public Service Law, etc.). **Details should be outlined in the Statement of Work prior to engagement of services.**


Samples are provided for discussion purposes only and are not intended as legal advice.
What provisions are included in existing State resources?

OGS Umbrella Contract

Appendix J: Contractor’s Insurance Requirements

• Data Breach and Privacy/Cyber Liability Insurance
• Technology Errors and Omissions Insurance
• Crime Insurance

Samples are provided for discussion purposes only and are not intended as legal advice.
### Appendix J: Contractor’s Insurance Requirements

**Data Breach and Privacy/Cyber Liability**

<table>
<thead>
<tr>
<th>Lot</th>
<th>Minimum Insurance Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lot 1 – Software</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>Lot 2 – Hardware</td>
<td>$1,000,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lot 3 – Cloud *</th>
<th>Minimum Insurance Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Risk</td>
<td>$2,000,000</td>
</tr>
<tr>
<td>Moderate Risk</td>
<td>$5,000,000</td>
</tr>
<tr>
<td>High Risk</td>
<td>$10,000,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lot 4 – Implementation</th>
<th>Minimum Insurance Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$1,000,000</td>
</tr>
</tbody>
</table>

*See NYS-S14-002 Information Classification Standard or successor available at [http://www.its.ny.gov/tables/technologypolicyindex.htm](http://www.its.ny.gov/tables/technologypolicyindex.htm) for additional information relating to risk categories. Contractor must maintain minimum insurance coverage for the level of risk for which Contractor provides Products and submit documentation in accordance with the terms of this Contract.

**Technology Errors and Omissions**

<table>
<thead>
<tr>
<th>Lot</th>
<th>Minimum Insurance Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lot 1 – Software</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>Lot 2 – Hardware</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>Lot 3 – Cloud *</td>
<td>$2,000,000, $5,000,000, $10,000,000</td>
</tr>
<tr>
<td>Lot 4 – Implementation</td>
<td>$1,000,000</td>
</tr>
</tbody>
</table>

Samples are provided for discussion purposes only and are not intended as legal advice.
Appendix J: Contractor’s Insurance Requirements

Crime Insurance: includes cyber theft if not provided as part of Cyber Liability

<table>
<thead>
<tr>
<th>Lot</th>
<th>Crime Insurance</th>
<th>Minimum Insurance Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lot 1 – Software</td>
<td></td>
<td>$2,000,000</td>
</tr>
<tr>
<td>Lot 2 – Hardware</td>
<td></td>
<td>$2,000,000</td>
</tr>
<tr>
<td>Lot 3 – Cloud</td>
<td>Low Risk</td>
<td>$2,000,000</td>
</tr>
<tr>
<td></td>
<td>Moderate Risk</td>
<td>$5,000,000</td>
</tr>
<tr>
<td></td>
<td>High Risk</td>
<td>$10,000,000</td>
</tr>
<tr>
<td>Lot 4 - Implementation</td>
<td></td>
<td>$2,000,000</td>
</tr>
</tbody>
</table>

*See NYS-S14-002 Information Classification Standard or successor available at [http://www.its.ny.gov/tables/technologypolicyindex.htm](http://www.its.ny.gov/tables/technologypolicyindex.htm) for additional information relating to risk categories. Contractor must maintain minimum insurance coverage for the level of risk for which Contractor provides Products and submit documentation in accordance with the terms of this Contract.

Samples are provided for discussion purposes only and are not intended as legal advice.

<table>
<thead>
<tr>
<th>INFORMATION CLASSIFICATION CATEGORIES</th>
<th>LOW</th>
<th>MODERATE</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CONFIDENTIALITY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consider impact of unauthorized disclosure on factors such as:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Health and Safety</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Financial Loss</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mission/Programs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Public Trust</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The unauthorized access or disclosure of information would have <strong>limited or no impact</strong> to the organization, its critical functions, workforce, business partners and/or its customers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The unauthorized access or disclosure of information would have <strong>serious impact</strong> to the organization, its critical functions, workforce, business partners and/or its customers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The unauthorized access or disclosure of PPSI or other information would have a <strong>severe or catastrophic impact</strong> on the organization, its critical functions, workforce, business partners and/or its customers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>INTEGRITY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consider impact of unauthorized modification or destruction of information on factors such as:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Health and Safety</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Financial Loss</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mission/Programs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Public Trust</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The unauthorized modification or destruction of information would have <strong>limited or no impact</strong> to the organization, its critical functions, workforce, business partners and/or its customers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The unauthorized modification or destruction of information would have <strong>serious impact</strong> to the organization, its critical functions, workforce, business partners and/or its customers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The unauthorized modification or destruction of information would have a <strong>severe or catastrophic impact</strong> on the organization, its critical functions, workforce, business partners and/or its customers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AVAILABILITY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consider impact of untimely or unreliable access to information on factors such as:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Health and Safety</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Financial Loss</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mission/Programs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Public Trust</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The disruption of access to or use of information would have <strong>limited or no impact</strong> to the organization, its critical functions, workforce, business partners and/or its customers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The disruption of access to or use of information would have <strong>serious impact</strong> to the organization, its critical functions, workforce, business partners and/or its customers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The disruption of access to or use of information would have a <strong>severe or catastrophic impact</strong> on the organization, its critical functions, workforce, business partners and/or its customers.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What provisions are included in existing State resources?

## ITS Contracts

- Warranties
- Indemnification
- State Data = Confidential Information
- Security Procedures & Employee Dishonesty
- Nondisclosure & Confidentiality
- Compliance with Information Security Policies & Procedures
- Employee training
- Limited Access to Data
- Security Measures; Encryption

- Access to State Facilities
- ISBNA
- Breach Reporting and Required Contractor Actions
- Data Transparency, Accessibility, Transport, Protection and Destruction
- Secure Development, Configuration & Lifecycle
- Security Review, Security Issue Management, and Assurance
- Federal, State, or Local Requirements
- CJIS, HIPAA, Pub 1075
- Hosting in the United States
- Disclosure of planned use of subcontractors
- Transition

Samples are provided for discussion purposes only and are not intended as legal advice
Where is there additional guidance?

- OGS “Information Technology Umbrella Contract – Manufacturer Based (Statewide)
  https://ogs.ny.gov/purchase/snt/awardnotes/7360022802can.HTM
- OGS “How to Use the Umbrella Manufacturer Contract”
  https://www.ogs.ny.gov/purchase/snt/awardnotes/7360022802HowToUse.pdf
- Center for Digital Government “Best Practice: Cloud and As-A-Service Procurements”
Where is there additional guidance?

Cybersecurity Legal Task Force Vendor Contracting Project: Cybersecurity Checklist:


NIST Special Publication 900-171r1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST Best Practices in Cyber Supply Chain Risk Management
Questions?

THANK YOU!