Adapting to the volatile cybersecurity landscape – knowledge, strategy, action for government contractors

March 2015
Contents/agenda

> Knowledge
  > Potential requirements for contractors
  > Impacted organizations
  > Risks of non-compliance
  > Looking ahead

> Strategy
  > Fitting it all together
  > Compliance planning

> Action
  > Implementing cybersecurity controls
## Knowledge: Potential Requirements for Contractors

<table>
<thead>
<tr>
<th>Requirement</th>
<th>What is Required</th>
<th>Primary Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFARS 252.204-7012</td>
<td>• Implement “minimum controls” for safeguarding information and systems</td>
<td>• NIST SP 800-53</td>
</tr>
<tr>
<td></td>
<td>• Report cyber incidents within 72 hours of discovery</td>
<td></td>
</tr>
<tr>
<td>Executive Order 13636</td>
<td>• Expand information sharing and collaboration between government and private sector</td>
<td>• NIST Cybersecurity Framework</td>
</tr>
<tr>
<td></td>
<td>• Develop a voluntary framework of cybersecurity standards and best practices</td>
<td></td>
</tr>
<tr>
<td>FedRAMP</td>
<td>• Meet security requirements to become authorized as a provider of cloud products or services</td>
<td>• FedRAMP.gov</td>
</tr>
<tr>
<td></td>
<td>• Accreditation by third-party assessment organization (3PAO)</td>
<td></td>
</tr>
<tr>
<td>FISMA</td>
<td>• Categorize information / systems by risk-level</td>
<td>• NIST SP 800-53</td>
</tr>
<tr>
<td></td>
<td>• Implement security controls</td>
<td>• OMB Circular A-130</td>
</tr>
<tr>
<td></td>
<td>• Develop System Security Plan (SSP)</td>
<td>• FIPS 199</td>
</tr>
<tr>
<td></td>
<td>• Certification, accreditation, and continuous monitoring</td>
<td></td>
</tr>
<tr>
<td>HIPAA</td>
<td>• Ensure privacy, security, and breach notification safeguards</td>
<td>• HHS.gov</td>
</tr>
<tr>
<td></td>
<td>• Ensure compliance by workforce</td>
<td>• 45 C.F.R. parts 160, 164</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIST SP 800 (series)</td>
</tr>
<tr>
<td>Requirement</td>
<td>Who is impacted</td>
<td>Agencies *</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>DFARS 252.204-7012</td>
<td>• All Department of Defense (DoD) contractors</td>
<td>• DoD agencies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NASA</td>
</tr>
<tr>
<td>Executive Order 13636</td>
<td>• Potentially any contractor</td>
<td>• Civilian agencies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DoD agencies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NASA</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>• Contractors who provide cloud services for the government</td>
<td>• Civilian agencies</td>
</tr>
<tr>
<td>FISMA</td>
<td>• Contractors storing and/or processing government data</td>
<td>• Civilian agencies</td>
</tr>
<tr>
<td></td>
<td>• Dependent upon contract requirements</td>
<td>• NASA</td>
</tr>
<tr>
<td>HIPAA</td>
<td>• All “covered entities” (e.g., health care providers, clearinghouses, health plans) and business associates</td>
<td>• Civilian agencies focused on healthcare (e.g., VA, HHS)</td>
</tr>
</tbody>
</table>

* Indicates agencies most likely to impose requirements on contractors; not intended to be all-inclusive
Knowledge: risks of non-compliance

- Poor security posture leads to higher risk of being breached
- Reputation damage (RSA)
- Loss of existing contracts (USIS)
- Preclusion from bidding on future contracts (i.e., debarment)
- Regulatory penalties (New York and Presbyterian Hospital / Columbia University)

Lessons Learned!
- Understand your specific contract requirements on cybersecurity
- Establish relationship with your agency representative (e.g., CISO)
Pending legislation

- New FAR rule “Basic Safeguarding of Contractor Information Systems” (Proposed); Part 2011-020

- NIST SP 800-171 “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (Draft)

- Personal Data Notification and Protection Act (Proposed)

Other considerations

- Evolving technology (i.e., new capabilities = new threats)

- Knowledge sharing and awareness - increasing presence of cybersecurity-focused “communities of practice”
Redundancies exist across various frameworks and standards.

Complying with one standard does not necessarily mean compliance with others (e.g., FISMA and FedRAMP).

Depending on contract, may need to implement controls from multiple requirements.

Identify redundant control requirements and document for future reference (e.g., develop cross-walk).

**Lessons Learned!**
- Avoid open sourced encryption technologies
- Collaboratively discuss alternative solutions with your CISO
Strategy: compliance planning

- Define specific regulatory and/or contractual cybersecurity requirements (i.e., future state)

- Assess current state policies, processes and procedures, and identify gaps

- Understand key contractual milestone dates for achieving compliance

- Engage third-parties (e.g., consultants, third-party assessors)

Lessons Learned!
- Involve internal IT/security personnel before you sign the contract
- Delays in addressing requirements may lead to loss of revenue
Action: implementing cybersecurity controls

01 Define system boundaries
02 Categorize information & information systems
03 Select and implement security controls
04 Assess security controls
05 Authorize information system
06 Monitor security controls
Action: implementing cybersecurity controls (cont’d)

> Key documentation includes:

>  > System Security Plan (SSP)

>  > Plan of Actions and Milestones (PoAM)

>  > Third-party assessment reports

Lessons Learned!

- Know your agency’s cybersecurity concerns and priorities
- Use agency-provided templates and tools to fullest extent possible
Cybersecurity resources

> Implementing an effective cybersecurity management program

> Manage mobile device risks holistically

> Read more about cybersecurity

Connect with us >> bakertilly.com
The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International. © 2015 Baker Tilly Virchow Krause, LLP.