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

March 2015

© Baker Tilly Virchow Krause, LLP

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

© Baker Tilly Virchow Krause, LLP

Knowledge: potential requirements for contractors

BAKER TILLY

Requirement	What is required?	Primary guidance
DFARS 252.204-7012	• Implement "minimum controls" for safeguarding information and systems • Report cyber incidents within 72 hours of discovery	• NIST SP 800-53
Executive Order 13636	• Expand information sharing and collaboration between government and private sector • Develop a voluntary framework of cybersecurity standards and best practices	• NIST Cybersecurity Framework
FedRAMP	• Meet security requirements to become authorized as a provider of cloud products or services • Accreditation by third -party assessment organization (3PAO)	• FedRAMP.gov
FISMA	• Categorize information / systems by risk-level • Implement security controls • Develop System Security Plan (SSP) • Certification, accreditation, and continuous monitoring	• NIST SP 800-53 • OMB Circular A-130 • FIPS 199
HIPAA	• Ensure privacy, security, and breach notification safeguards • Ensure compliance by workforce	• HHS.gov • 45 C.F.R. parts 160, 164 • NIST SP 800 (series)

© Baker Tilly Virchow Krause, LLP

Knowledge: impacted organizations

BAKER TILLY

Requirement	Who is impacted?	Agencies *
DFARS 252.204-7012	• All Department of Defense (DoD) contractors	• DoD agencies • NASA
Executive Order 13636	• Potentially any contractor	• Civilian agencies • DoD agencies • NASA
FedRAMP	• Contractors who provide cloud services for the government	• Civilian agencies
FISMA	• Contractors storing and/or processing government data • Dependent upon contract requirements	• Civilian agencies • NASA
HIPAA	• All "covered entities" (e.g., health care providers, clearinghouses, health plans) and business associates	• Civilian agencies focused on healthcare (e.g., VA, HHS)

**** Indicates agencies most likely to impose requirements on contractors; not intended to be all-inclusive***

© Baker Tilly Virchow Krause, LLP

Knowledge: risks of non-compliance

BAKER TILLY

- 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)

© Baker Tilly Virchow Krause, LLP

Knowledge: looking ahead

- 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”

© Baker Tilly Virchow Krause, LLP

Strategy: fitting it all together

BAKER TILLY

- 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

© Baker Tilly Virchow Krause, LLP

Strategy: compliance planning

BAKER TILLY

- 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

© Baker Tilly Virchow Krause, LLP

Action: implementing cybersecurity controls

© Baker Tilly Virchow Krause, LLP

Action: implementing cybersecurity controls (cont'd)

BAKER TILLY

- 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

© Baker Tilly Virchow Krause, LLP

BAKER TILLY

Cybersecurity resources

- *Implementing an effective cybersecurity management program*
- *Manage mobile device risks holistically*
- *Read more about cybersecurity*

Connect with us >> bakertilly.com

© Baker Tilly Virchow Krause, LLP

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.