
REFORMING THE MODEL PROCUREMENT CODE
FREE ONLINE SUMMER SERIES
JULY 18, 20, 25, and 27
6-8 PM EST
GW LAW

Welcome

Professor Christopher Yukins
GW Law School – Government Procurement Law Program

- Recording and materials at www.publicprocurementinternational.com
- Questions & Answers (Q&A)
- All speakers' statements are in their personal capacities

Cybersecurity Overview

What is Cybersecurity?

- Information Security
- Systems Security
- Operational Security
- Privacy

Federal Cybersecurity Standards

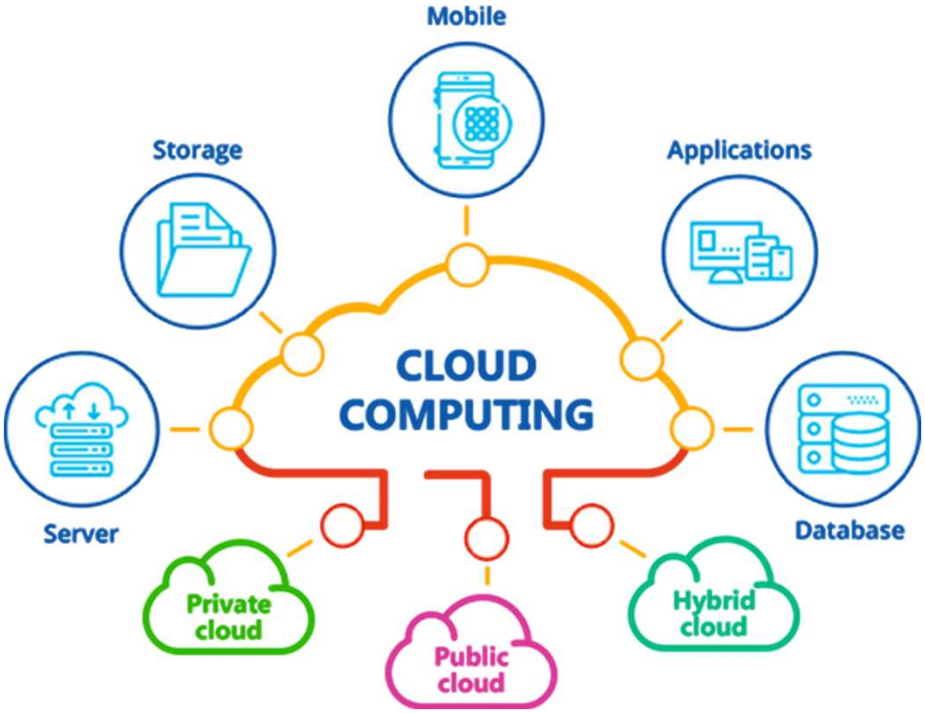
The CUI Program

- 32 C.F.R. Part 2002
  - Marking CUI
  - Handling CUI
  - Information Systems Requirements
- FAR Subpart 4.19 Basic Safeguarding of Covered Contractor Information Systems
  - Clause 52.204-21
- Agency Supplements
- Assessment & Validation

CONTROLLED
UNCLASSIFIED
INFORMATION

Cloud-Based Services: FedRAMP®

- Federal government has prioritized cloud-based services since 2010
- The Federal Risk and Authorization Management Program (FedRAMP®) manages through the GSA cloud service providers
- Certification is issued to providers following assessments
- Various impact levels depending on information managed
- Enforced through service level agreements



Total FedRAMP Authorized Services

313

State and Local Government Cybersecurity Grants

- OMB Guidance: “reasonable measures” to protect information
- Example: DC Police ransomware attack
- Opportunities for states to adopt new security standards in acquisitions
- Cyber Response & Recovery Fund

Procurement Codes and Cybersecurity

Comparing State Cybersecurity Requirements

Connecticut

- CONN. GEN. STAT. ANN. § 4d-2 (West 2023)
- Creates Department of Information Technology within Department of Administrative Services led by CIO
- Protects “Public Record”
- Contains reporting and enforcement provisions
- Does not mention cybersecurity, last amended 2012

New Jersey

- N.J. ADMIN. CODE § 5:34-5.1 *et seq.* (2023)
- Covers cybersecurity standards for procurement platforms concerning local public schools
- More modern, refers to FedRAMP, NIST password standards
- Mandatory reporting provisions
- Standards are for platform, not contractors

Examples of Statutes Within Procurement Codes

- MD. CODE ANN., STATE FIN. & PROC. § 13-115 (West 2023)
- MD. CODE ANN., STATE FIN. & PROC. § 4-308 (West 2023)
- 30 ILL. COMP. STAT. ANN. 500/25-90 (West 2023)

30 Ill. Comp. Stat. Ann. 500/25-90 (West 2023)

§ 25-90. Prohibited and authorized cybersecurity products. State agencies are prohibited from purchasing any products that, due to cybersecurity risks, are prohibited for purchase by federal agencies pursuant to a United States Department of Homeland Security Binding Operational Directive. However, a State agency or public institution of higher education may purchase those offerings that are included in the Authorized Product List maintained by StateRAMP and that have been verified by StateRAMP as having an authorized security status.

Cybersecurity Outside of Procurement Codes

An Alternative Approach to Standards

- More states are instead creating IT Departments led by a CIO or equivalent
- General theme is they are separated from the Procurement function but have the ability to oversee relevant contracts
- Gives control of cybersecurity standards to experienced individual

NM DEPARTMENT OF INFORMATION TECHNOLOGY

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

utah govops division of Technology Services

Examples of IT Department Standards

- UTAH CODE ANN. § 63A-16-201 *et seq.* (West 2023)
  - Creates a Chief Information Officer and their function
- N.M. STAT. ANN. § 9-27-6 (West 2023)
  - Designates powers and duties of the secretary
- N.C. GEN. STAT. § 143B-1350 (2023)
  - Section dedicated to procurement of information technology
- OHIO REV. CODE ANN. § 125.18 (West 2023)
  - Establishes Office of Information Technology within Department of Administrative Services
- OR. ADMIN. R. 125-800-0020 (2023)
  - Empowers Department of Administrative Services to be primary player in information security
- FLA. ADMIN. CODE. ANN. r. 60GG-2.002 (2023)
  - Sets out Florida's cybersecurity standards, including contracting requirements

Statute Excerpts

- As chief information officer, the secretary shall: (4) approve agency information technology contracts and amendments to those contracts, including emergency procurements, sole source contracts and price agreements, prior to approval by the department of finance and administration (N.M. STAT. ANN. § 9-27-6(C)(4) (West 2023))
- (h) All offers to contract, whether through competitive bidding or other procurement method, shall be subject to evaluation and selection by acceptance of the most advantageous offer to the State. Evaluation shall include best value, as the term is defined in G.S. 143-135.9(a)(1), compliance with information technology project management policies, **compliance with information technology security standards and policies**, substantial conformity with the specifications, and other conditions set forth in the solicitation. (N.C. GEN. STAT. § 143B-1350 (2023))

TX-RAMP and AZRAMP

- Texas and Arizona have both created their own certification method for authorized vendors
- Texas utilizes 2 levels of security as its baseline
- Authorized products lists exist for both
- Both programs accept StateRAMP/FedRAMP certification in place of state's process

Contract Clauses

- Cybersecurity standards can be directly implemented into contracts, California being a key example
- Has three relevant contracts
- General Provisions - Information Technology
- GENERAL PROVISIONS – INFORMATION TECHNOLOGY – CLOUD COMPUTING – SOFTWARE as a SERVICE (SaaS)
- STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service and Platform as a Service)

Language from Contracts

- CONFIDENTIALITY OF DATA: All financial statistical, personal, technical and other data and information relating to the State's operation which are designated confidential by the state and made available to the Contractor in order to carry out this Contract, or which become available to the Contractor in carrying out this Contract, shall be protected by the Contractor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State. (General IT Provisions)
- The Service Provider shall provide its services to the State and its end users solely from data centers in the continental United States. Storage of State Data at rest shall be located solely in data centers in the continental United States. (IaaS and PaaS)

Enforcing Cybersecurity

Federal Enforcement of Cybersecurity in Government Contracts

Jelly Bean Communications Design LLC

- False Claims Act action led to $293,771 settlement
- (Contractor?) Florida's Healthy Kids Corp. contracted with Jelly Bean communications for web design and support
- The agreement provided that Jelly Bean would adapt, modify, and create the necessary code to support the secure communication of data.
- Allegations centered around failure to provide secure hosting of personal information, 500,000 applications allegedly hacked

iHealth Solutions, LLC

- HIPAA investigation by Department of Health and Human Services' Office for Civil Rights ends with $75,000 settlement
- iHealth provides coding, billing, and onsite information technology services to healthcare providers
- Data breach allegedly occurred when network server containing the protected health information of 267 people was left unsecured on the internet

New York Department of Financial Services Enforcing Cybersecurity Standards (23 NYCRR Part 500)

OneMain Financial Group LLC

- Penalty of $4.25 million leveled against OneMain, a licensed lender and mortgage servicer
- Company allegedly failed to manage third-party service provider risk, manage access privileges, and other vulnerabilities
- Allegedly failed to utilize formal methodology in addressing software development, increasing vulnerability

EyeMed Vision Care LLC

- EyeMed, a licensed health insurance company, is forced to pay a $4.5 million penalty
- Allegedly collected non-public health data that was exposed following a phishing attack, affecting hundreds of thousands of people
- Alleged issue was failure to utilize multi-factor authentication and allowing employees to share credentials

Conclusion

- Cybersecurity issues are a problem that needs to be addressed in government procurement as technology evolves
- Certification programs that already exist can help state governments with catching up if needed
- Cybersecurity approaches from other sectors of the government can be used as templates for reform