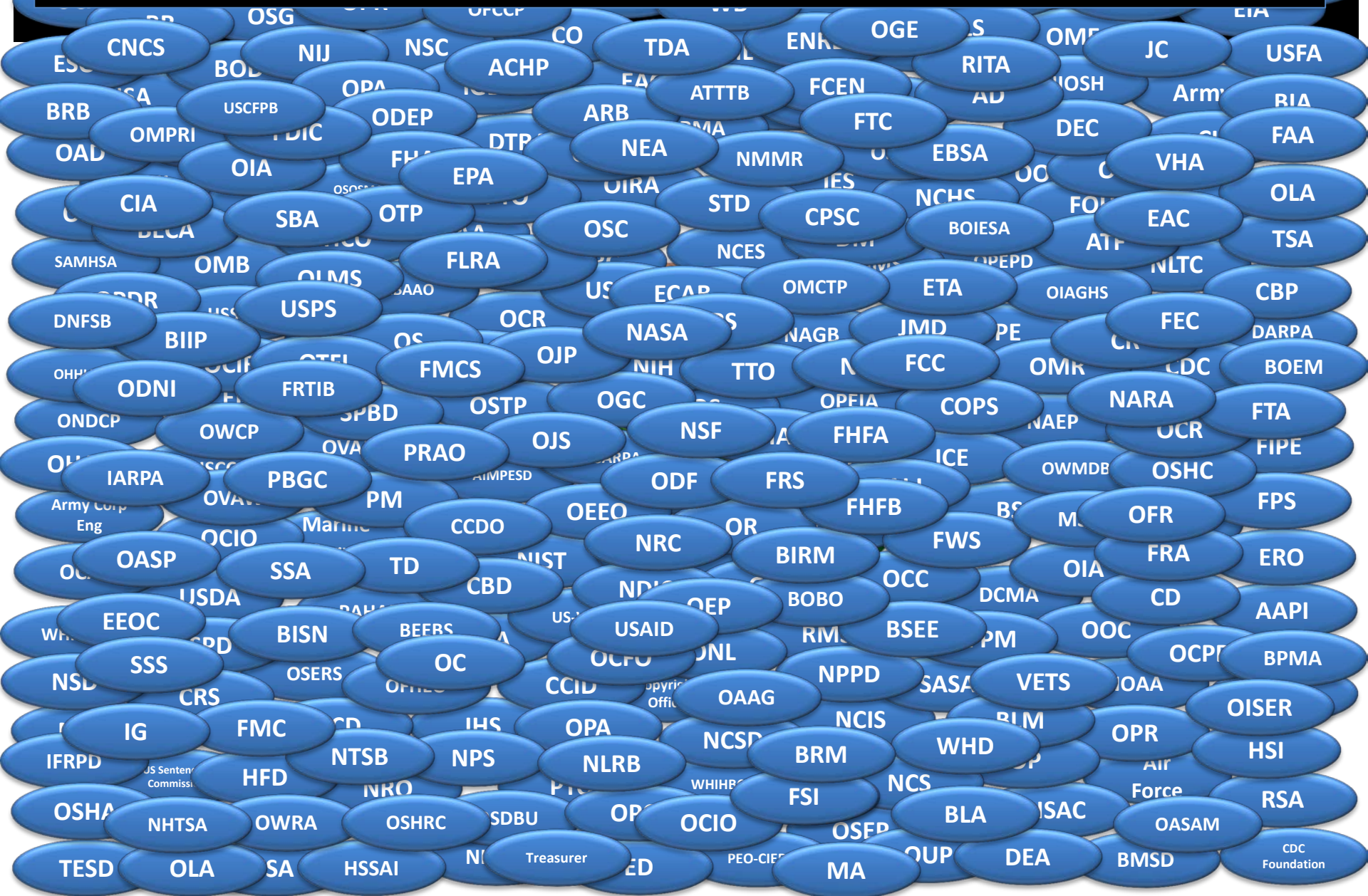


Intersections between Privacy & Security Contracts: Your Best Defense

Roslyn F. Martorano
Systemwide Privacy Manager

UC | Legal Obligations & Regulators



Innovation Takes a Village... and Strong Contracts

Great benefits of using vendors:

- Lowers cost
- More robust solutions that can be implemented faster
- Perform reporting functions we cannot



And some drawbacks:

- Vendors are responsible for **42%** of all security breaches
- Sell or use data without our permission or oversight
- Act, but leave UC paying the fines or penalties



Harm? What Harm?

California requires that UC contractually bind vendors to protect personal information.

UC contracts outline:

- Access, collection, use
- Retention and disposition
- Breaches
- Liability
- Protection (security considerations like storage, format maintenance, encryption)



Risk-based decisions are critical.

Source: (Cal. Civ. Code 1798.81.5(c))

Be Strong, Sign a Contract

1. Some privacy and security issues are not negotiable. Be prepared to walk away.
2. It's not always obvious if a contract relates to data:
 - Be on the lookout
 - Don't forget about free and low cost services
3. Use UC contract templates and negotiate as a united location with potential vendors
4. Make sure it's "good enough" for UC, *not* another University



Questions?

Contact your local privacy or information security professional:

Campus Privacy Officials	http://www.ucop.edu/ethics-compliance-audit-services/compliance/privacy/campus-privacy-officials.html
Campus Information Security Officials	http://www.ucop.edu/information-technology-services/initiatives/it-policy-and-security/itps-members.html
HIPAA Privacy Officials	http://www.ucop.edu/ethics-compliance-audit-services/compliance/hipaa/hipaa-privacy-compliance.html
HIPAA Security Officials	http://www.ucop.edu/ethics-compliance-audit-services/compliance/hipaa/hipaa-security-compliance.html