About the Speaker

Education and Certification
- BS, MS in Information Assurance, University of Nebraska Omaha
- Certified Information Systems Security Professional, CISSP
- GIAC Law of Data Security & Investigations, GLEG

Experience
- Information Security Analyst and Authorizing Official, Boys Town
- Nuclear and Space Mission Systems Cybersecurity Analyst, U.S. Strategic Command
- National and Nuclear Command and Control Enterprise and Solutions Architect

Distinctions
- Joint Civilian Service Achievement Award (2015)
- C4 Systems Directorate Civilian of the Quarter (2011, 2014)
- Walter Scott, Jr. Scholarship (2008)
Agenda

- Identification of Applicable Laws and Regulations
- Information Security Register
- Review of Cybersecurity Law
  - International Laws
  - Federal Laws
  - State Laws
  - Industry Regulations
- Integration with the Risk Management Framework
Identification of Applicable Laws and Regulations
Identification of Applicable Laws and Regulations

- Identify Sources
  - Regulated Industries
  - Legal Jurisdictions
  - Protected Information Types

- Identify Regulators
  - International
  - Federal
  - State
  - Industry
Regulated Industries

- Identify all known industries your organization operates in
  - Think about what products/services you provide
  - Think about what departments you have

- Think broad, then focus in
  - Ex., A bank’s industries may include banking, finance (loans), investments, insurance, and storage (safety deposit boxes)

- Major regulated industries:
  - Healthcare
  - Education
  - Infrastructure
  - Finance
  - Commerce
Legal Jurisdictions

- Identify all known legal jurisdictions you operate in
  - Think about where your offices/branches are
  - Think about where your customers live
  - Think about where your interactions with customers are
    - Brick-and-Mortar and Online
- Goal is to identify all countries and states you operate in
Protected Information Types

- Determine **intuitive** types of information
  - Ex. Cardholder data, medical records, etc.

- Determine **formal** types of information
  - Reference the Federal Enterprise Architecture and NIST SP 800-60 Volume I and II
    - May require minor tailoring from federal focus
  - Ensures you capture most exception cases
  - **Bonus:** NIST maps FEA information types to C-I-A impact for security control selection
## Protected Information Types

<table>
<thead>
<tr>
<th>Information Types</th>
<th>Security Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Personally Identifiable Information</td>
<td>Moderate</td>
</tr>
<tr>
<td>Protected Health Information</td>
<td>Low</td>
</tr>
<tr>
<td>Consumer Financial Information / NPI</td>
<td>Low</td>
</tr>
<tr>
<td>Private &amp; Foundation Grants</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Knowledge Creation and Management</strong></td>
<td></td>
</tr>
<tr>
<td>Research &amp; Development</td>
<td>Low</td>
</tr>
<tr>
<td>General Purpose Data &amp; Statistics</td>
<td>Low</td>
</tr>
<tr>
<td>Advising &amp; Consulting</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Public Affairs</strong></td>
<td></td>
</tr>
<tr>
<td>Product Outreach</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Information &amp; Technology Management</strong></td>
<td></td>
</tr>
<tr>
<td>Record Retention</td>
<td>Moderate</td>
</tr>
<tr>
<td>Information Sharing</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Security Categorization</strong></td>
<td>Moderate</td>
</tr>
</tbody>
</table>
Regulators

- Identify all regulators that have jurisdiction over you
  - Consider regulators who have conducted past audits
  - Consider regulators who audit similar organizations
  - Consider regulators who issue guidance in your industry

- Identify which laws/regulations those regulators focus on
  - Typically based on past findings, cases against other organizations
  - Some, like FTC, list their core areas on their website
Information Security Register
The Register

- The Register is your cybersecurity *body of knowledge*
  - Document and maintain for posterity
- Excel workbook with the following sheets
  - **Regulations**: document all applicable laws/regulations
  - **Systems**: document all information systems
  - **Controls**: document all sets of security control selections
  - **Definitions**: document all acronyms and definitions
  - **Exclusions**: document all non-applicable laws/regulations, with justifications
  - **Read Me**: document basic information about the workbook
## The Register: Regulations Tab

<table>
<thead>
<tr>
<th>Regulation Name</th>
<th>Total: 280</th>
<th>Requirements</th>
<th>Penalties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybersecurity Law Register</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BSA</strong></td>
<td>Federal</td>
<td>§ 5321(a)(2); Financial institutions; Maintain records about reportable transactions for 6 years</td>
<td>Fine not to exceed $100K per day, per location</td>
</tr>
<tr>
<td><strong>CAN-SPAM</strong></td>
<td>Federal</td>
<td>§ 5321(b); Prohibition of false or misleading transmission information; prohibition of deceptive subject headings; inclusion of return address or comparable mechanism (unsubscribe link); allowance to provide detailed unsubscribe; prohibition of transmission of commercial email after objection (unsubscribe) after 10 business days; inclusion of identifier, opt-out, and physical address; prohibition of address harvesting and dictionary attacks; requirement to place warning labels on emails containing sexually oriented material</td>
<td>$250 per email not to exceed $200K; may be blacklisted by ISPs until compliant</td>
</tr>
<tr>
<td><strong>CFATS</strong></td>
<td>Federal</td>
<td>§ 21.136; Chemical facilities and covered facilities (energy and utilities, agriculture and food, healthcare)</td>
<td></td>
</tr>
<tr>
<td><strong>CIPA</strong></td>
<td>Federal</td>
<td>§ 27.105; Maintain records for 3 years</td>
<td></td>
</tr>
<tr>
<td><strong>CJIS</strong></td>
<td>Federal</td>
<td>§ 27.406; Protect and mark CVI classified information</td>
<td></td>
</tr>
<tr>
<td><strong>COPPA</strong></td>
<td>Federal</td>
<td>§ 312.3; Notice on website of privacy policy; obtain parental consent; means for review of information and refusal to continue by parents; establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of child's information; § 312.4; Require reasonable security from third-parties who obtain the data; § 312.56; Only retain as long as needed; delete using measures to protect against unauthorized access to or use of information during the deletion process</td>
<td>$11K–$16K per violation</td>
</tr>
<tr>
<td><strong>Cybersecurity Law Register</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CIPA</strong></td>
<td>Federal</td>
<td>§ 27.105; Maintain records for 3 years</td>
<td></td>
</tr>
<tr>
<td><strong>CJIS</strong></td>
<td>Federal</td>
<td>§ 27.406; Protect and mark CVI classified information</td>
<td></td>
</tr>
<tr>
<td><strong>COPPA</strong></td>
<td>Federal</td>
<td>§ 312.3; Notice on website of privacy policy; obtain parental consent; means for review of information and refusal to continue by parents; establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of child's information; § 312.4; Require reasonable security from third-parties who obtain the data; § 312.56; Only retain as long as needed; delete using measures to protect against unauthorized access to or use of information during the deletion process</td>
<td>$11K–$16K per violation</td>
</tr>
<tr>
<td><strong>COPPA</strong></td>
<td>Federal</td>
<td>§ 312.3; Notice on website of privacy policy; obtain parental consent; means for review of information and refusal to continue by parents; establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of child's information; § 312.4; Require reasonable security from third-parties who obtain the data; § 312.56; Only retain as long as needed; delete using measures to protect against unauthorized access to or use of information during the deletion process</td>
<td>$11K–$16K per violation</td>
</tr>
<tr>
<td>System Name</td>
<td>Information System Security Engineer</td>
<td>Security Control Assessor</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name: Title: Department: Location:</td>
<td>Name: Title: Department:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone Number: Email:</td>
<td>Location: Phone Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Email:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Name</th>
<th>Information System Security Engineer</th>
<th>Security Control Assessor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name: Title: Department: Location:</td>
<td>Name: Title: Department:</td>
</tr>
<tr>
<td></td>
<td>Phone Number: Email:</td>
<td>Location: Phone Number:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Email:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Name</th>
<th>Information System Security Engineer</th>
<th>Security Control Assessor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name: Title: Department: Location:</td>
<td>Name: Title: Department:</td>
</tr>
<tr>
<td></td>
<td>Phone Number: Email:</td>
<td>Location: Phone Number:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Email:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Name</th>
<th>Information System Security Engineer</th>
<th>Security Control Assessor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name: Title: Department: Location:</td>
<td>Name: Title: Department:</td>
</tr>
<tr>
<td></td>
<td>Phone Number: Email:</td>
<td>Location: Phone Number:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Email:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Name</th>
<th>Information System Security Engineer</th>
<th>Security Control Assessor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name: Title: Department: Location:</td>
<td>Name: Title: Department:</td>
</tr>
<tr>
<td></td>
<td>Phone Number: Email:</td>
<td>Location: Phone Number:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Email:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational Status</th>
<th>Information System Type</th>
<th>Authorization Status</th>
<th>Authorization Date</th>
<th>System Categorization</th>
<th>Last Assessed Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Register: Systems Tab
<table>
<thead>
<tr>
<th>Control Number</th>
<th>Control Name</th>
<th>NIST SP 800-53</th>
<th>NIST SP 800-171</th>
<th>CIS CC</th>
<th>CGCS</th>
<th>ENISA 3255</th>
<th>ENISA 3255 Risk Rating Controls Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access Control Policy and Procedures</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2-2</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2-3</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2-4</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2-6</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2-8</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2-10</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2-11</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2-12</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2-13</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2-15</td>
<td>Account Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>Access Enforcement</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Review of Cybersecurity Law
Cybersecurity Law

- Laws and regulations exist to protect our rights and prevent unfair and deceptive practices
  - If you are non-compliant with the law, you are breaking it

- Strategic Questions
  - What cybersecurity laws must you comply with?
  - What is your exposure if you are non-compliant?
  - What organizations regulate/audit you?
  - How do you manage all of these requirements?
International Laws

- Two basic legal approaches
  - Common Law - U.S. and U.K.
  - Civil Law - Continental Europe
- E.U. General Data Protection Regulation (GDPR)
  - Applies to any E.U. citizen’s PII
  - Applies to any websites accessible in E.U.
GDPR: €10,000,000 Finable Offenses

Information Security

Article 25: Data Protection by Design and by Default
Article 30: Records of Processing Activities (security plans)
Article 32: Security of Processing (reasonable and appropriate)
Article 33: Notification of a Personal Data Breach to the Supervisory Authority
Article 34: Communication of a Personal Data Breach to the Data Subject
Article 35: Data Protection Impact Assessment
Article 36: Prior Consultation (for high risk systems)
Article 39: Tasks of the Data Protection Officer
Executive Leadership
- Article 27: Representatives of Controllers or Processors Not Established in the Union
- Article 31: Cooperation with the Supervisory Authority
- Article 37: Designation of the Data Protection Officer
- Article 38: Position of the Data Protection Officer

Legal Department
- Article 26: Joint Controllers *(third-party contracts)*
- Article 28: Processor *(specific contract language)*

Support Staff
- Article 8: Conditions Applicable to Child’s Consent in Relation to Information Society Services
- Article 11: Processing Which Does Not Require Identification
- Article 29: Processing Under the Authority of the Controller or Processor
GDPR: €20,000,000 Finable Offenses

Information Security
- Article 44: General Principle for Transfers

Legal Department
- Article 12: Transparent Information, Communications and Modalities for the Exercise of the Rights of Data Subjects (transparency)

Support Staff
- Article 6: Lawfulness of Processing (opt-in)
- Article 7: Conditions for Consent
- Article 9: Processing of Special Categories of Personal Data (opt-in)
- Article 49: Derogations for Specific Situations
Federal Laws

- Two basic legal approaches
  - Laws primarily focused on cybersecurity
  - Laws focused on industry regulation with a security component
- Some laws apply to any organization conducting business
  - Discovery laws, trade laws, etc.
- Some apply to only certain categories of businesses
  - Operate across state lines, critical infrastructure, etc.
Federal Laws

Cybersecurity
- 42 CFR Part 2
- CFATS
- CIPA
- CJIS
- COPPA
- FDA 21 CFR Part 11
- FERPA
- FISMA
- HIPAA
- HITECH
- SEC Regulations S-P, S-AM, S-ID

Industry Regulation
- BSA
- CAN-SPAM
- Dodd-Frank
- EFTA
- FAA
- FACTA
- FCRA
- FCUA
- FDCPA
- FDIC
- FTC
- GLBA
- PAMA
- PPRA
- PREA
- SOX
- TCPA
- TILA

Business Regulation
- 4th Amendment to the U.S. Constitution
- ADA
- ADEA
- EPA
- ERISA
- FLSA
- FMLA
- FRCP
- GINA
- IRCA
- IRC
- OSHA
- Title VII
Health Insurance Portability and Accountability Act

- **Code**: 45 C.F.R. Part 160
- **Regulator**: U.S. Department of Health and Human Services
- **Scope**: Health care providers
- **Requirements**: Reasonable administrative, technical, and physical safeguards; electronic signatures; policy and procedure; breach notification; privacy policy disclaimer; record access; (specific requirements outlined in law text)
- **Penalties**: $100 per violation not to exceed $25K; $50K-$250K and up to 10 years imprisonment for wrongful disclosure
Dodd-Frank (for now...)

- **Code:** Pub.L. 111-203, H.R. 4173
- **Regulator:** Consumer Financial Protection Bureau and the U.S. Securities and Exchange Commission
- **Scope:** Mortgage lenders, credit/debit card issuers, investment bankers
- **Requirements:** Prevent unfair, deceptive, and abusive practices, including misrepresentation of data security practices; develop, implement, and maintain a comprehensive written information security plan; property train employees and fix security flaws; annually obtain an independent data security program audit
- **Penalties:** Civil penalties not more than the greater of $1M or 3x the monetary gain to such person for each violation
State Breach Notification Laws

- Three basic legal approaches
  - Collecting personal information about citizens of the state
  - Conducting business within the state
  - No breach notification law
- In general, most organizations *probably* collect information about citizens from every state
- In general, most organizations that conduct business online *probably* conduct business within every state
State Breach Notification Laws

Collecting PII about citizens
- Alaska
- Arkansas
- California
- Florida
- Georgia
- Hawaii
- Illinois
- Indiana
- Iowa
- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Missouri
- Nebraska
- Nevada
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- Tennessee
- Texas
- Utah
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- District of Columbia
- Guam
- Puerto Rico
- U.S. Virgin Islands

Conducting business in state
- Arizona
- Colorado
- Connecticut
- Delaware
- Idaho
- Kansas
- Minnesota
- Mississippi
- Montana
- New Hampshire
- New Jersey
- South Carolina
- Wyoming

No breach notification law
- Alabama
- South Dakota
- American Samoa
- Northern Mariana Islands
California

- Most progressive state in terms of cybersecurity laws
  - While most states have breach notification, California has at least 30 laws that have cybersecurity requirements
  - “Recommendation 1: The 20 controls in the CIS Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.” - California Attorney General Kamala D. Harris
Honorable Mentions

- Massachusetts “Standards for the Protection of Personal Information of Residents of the Commonwealth” outlines specific controls to implement
- Nevada “Security of Personal Information” requires compliance with PCI-DSS for all payment card transactions
- Rhode Island “Identity Theft Protection Act of 2015” requires a risk-based information security program
Industry Regulations

- Mandatory Regulations
  - Required by third-parties and contractual obligation
  - Ex., credit card processors require PCI-DSS compliance

- Voluntary Regulations
  - Provide competitive advantage through assurance
  - Ex., Good Housekeeping Seal of Approval
The Joint Commission Standards

- **Regulator:** The Joint Commission
- **Scope:** Accredited health care organizations
- **Requirements:** Information management; continuity of information management; protect privacy of health information; maintain security and integrity of health information; effectively manage the collection of health information; knowledge-based information resources are available, current, and authoritative
- **Penalties:** Loss of accreditation
North American Electric Reliability Corporation Standards

- **Regulator**: North American Electric Reliability Corporation
- **Scope**: Power production on public grids
- **Requirements**: Critical cyber asset identification; security management controls; personnel training; electronic security perimeters; physical security; systems security management; incident response; disaster recovery
- **Penalties**: $1M per violation per day
Payment Card Industry Data Security Standard

- **Regulator:** Payment Card Industry Security Standards Council
- **Scope:** Accepting payment cards from American Express, Discover, JCB, MasterCard, or Visa
- **Requirements:** Firewall; no default passwords; protect data-at-rest and data-in-transit; antivirus; develop secure systems and applications; access control need-to-know; unique user IDs; restrict physical access; monitor network access; test security systems/processes; maintain information security policy
- **Penalties:** $50-$90 per cardholder data breached; $5K-$100K per month of breach; loss of ability to accept PCI-sponsored credit cards
Integration with the Risk Management Framework
Risk-Based Security Program

- Risk-based information security program
  - Compliance ≠ Security
  - Reasonable and appropriate
  - Considers cost-benefit but not primary motivation

- Risk Management Framework
  - Mandated by Federal Information Security Management Act (FISMA)
  - Satisfies many federal, state, and industry requirements
  - National standards maintained by NIST under the Department of Commerce
Risk Management Framework

- Cost-effective, risk-based decision making
- Continuous monitoring of information system risk
- Strategic, operational, and tactical risk management
- Standardized process for assessing risk across information systems and operational lines of business
- Tailorable to any industry and regulatory environment
Security Maturity

- Ad Hoc
  - No Program
  - No Policy
  - Unknown Risk

- Triage
  - Reactive

- Compliant
  - Federal Law
  - State Law
  - Industry Regulation

- Best Practice
  - Proactive

- Security Culture
  - Awareness
  - Participation
  - Managed Risk
Questions?