## Project Manager User Group



# Project Management and Security

May19, 2021

***Bryant Lister, CISSP, PMP***

DHS
Oregon Department of Human Services

OFFICE OF INFORMATION SERVICES
Information Security & Privacy Office

Oregon Health Authority

# Bryant Lister is the Chief Information Risk Officer from ODHS/OHA



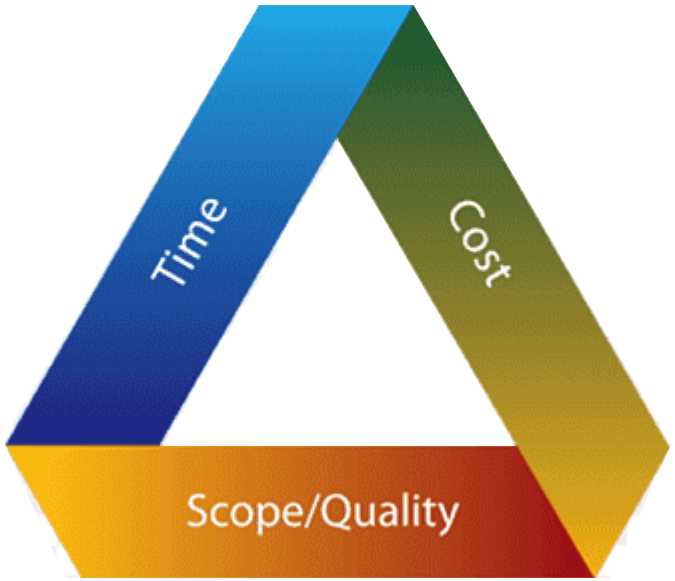
- Received PMP about 8 years ago
- Received CISSP early in 2020 (right before pandemic shutdown)
- Been an application developer, system analyst, project manager, development manager, strategic manager
- Director of the Information Security & Privacy Office in the Office of Information Services for ODHS/OHA

# What we will discuss today

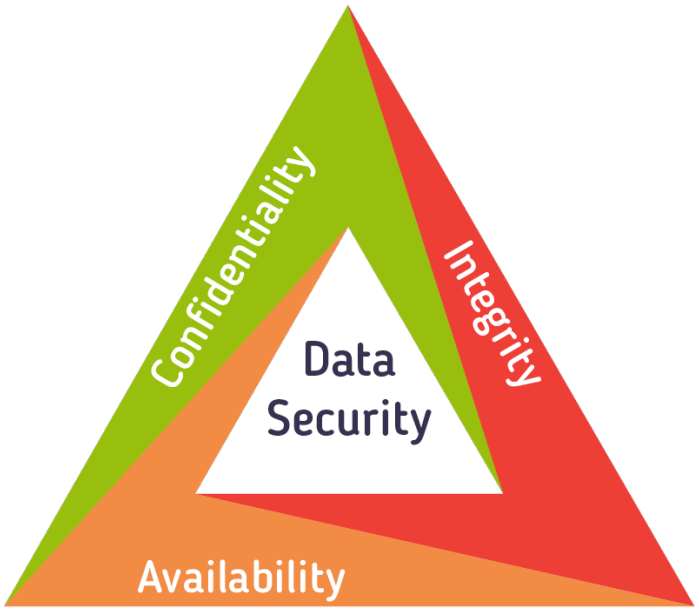
- Project Management & Security Triangles
- Shift Left
  - Project Phases – where does Security fit in?
  - Project Documents – writing about Security
    - Security Controls
    - Security Standards & Frameworks
      - Regulatory Bodies & Data Types
      - Data Acronyms & Terms
        - Risk Management
        - Consequences of not shifting left
          - Resources

# Triangles

## Project Management

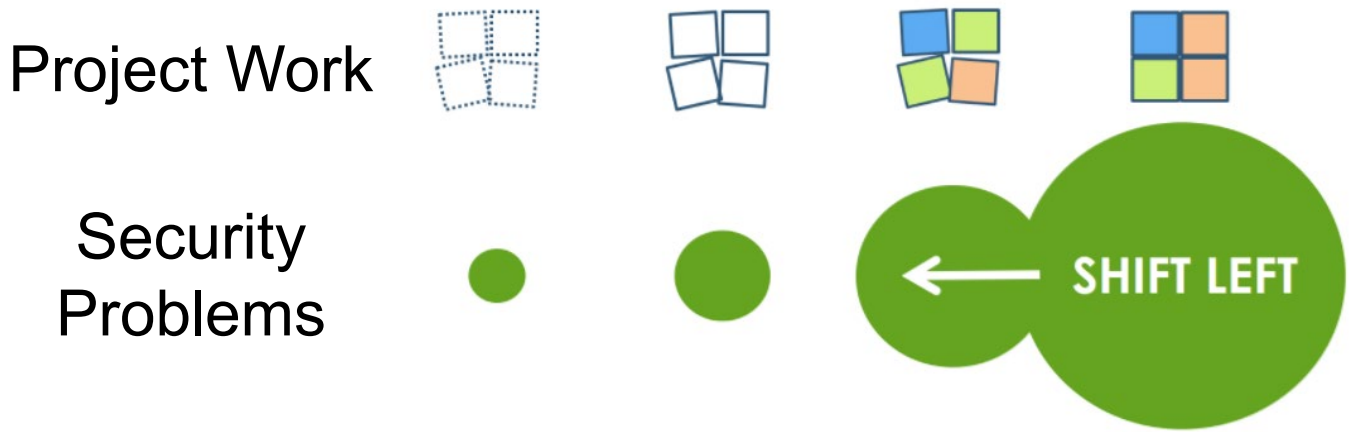



## Security



# Shift Left

- Setup projects securely
- Security issues should be identified early
- Less cost to address/fix when found at the beginning
- Security incidents can have extreme costs



# Project Phases – where does Security fit in?


There is a role for security in every phase

- Scope – what overall level of security is needed?
- Requirements – detailed security plans and needs
- Implementation – apply security controls, test for vulnerabilities
- Reports – security findings, access controls
- End – remove security rights for project team

# Project Documents – writing about Security

Standard docs

- Scope
- Plans
- Requirements
- WBS
- Schedule
- Contracts/Agreements
- Quality Metrics
- Risk Register

Special docs

- PIA
- POAM
- SSP

# Security Controls

**PHYSICAL CONTROLS**

- Doors
- Cameras
- Card readers

**TECHNICAL CONTROLS**

- Firewalls
- Passwords
- Encryption

**ADMINISTRATIVE CONTROLS**

- Policies
- Standards
- Data classification

# Security Standards & Frameworks

Statewide Information and Cyber Security Standards

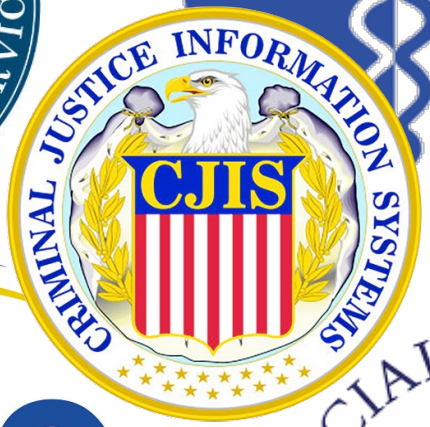
- Created by Enterprise Information Services

Security Control frameworks

- National Institute of Standards and Technology (NIST)
- Center for Internet Security (CIS) Critical Security Controls
- Control Objectives for Information and Related Technology (COBIT)
- International Standards Organization (ISO)

# Regulatory Bodies & Data Types


HIPAA
Health Insurance Portability & Accountability Act




CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES


# Data Acronyms & Terms

- PII, PCI, PHI, FTI
- Data Levels 1, 2, 3, 4
- Inference
- Obfuscation

| Level | 1 - Published | 2 - Limited | 3 - Restricted | 4 - Critical |
|---|---|---|---|---|
| **Risk Sensitivity** | Low | Sensitive | High | Extreme |
| **Policy 107-004-050 Definition** | Information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of agency employees, clients, and partners. This includes information regularly made available to the public via electronic, verbal, or hard copy media. | Information that may be protected from public disclosure, but if made easily and readily available, may jeopardize the privacy or security of agency employees, clients, or partners. Agency shall follow its disclosure policies and procedures before providing this information to external parties. | Information intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners, or individuals who otherwise qualify for an exemption. Information may be accessed and used by internal parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized agency business may be under contractual obligation of confidentiality with the agency prior to receiving it. | Information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the name individual(s), agency employees, clients, partners, or cause major harm to the agency. |
| **Policy Examples** | • Press releases<br>• Brochures<br>• Pamphlets<br>• Public access web pages<br>• Materials created for public consumption | • Enterprise risk management planning documents<br>• Published internal audit reports<br>• Names and addresses that are not protected from disclosure | • Network diagrams<br>• Personally identifiable information<br>• Other information exempt from public records disclosure | • Disclosure that could result in loss of life, disability, or serious injury<br>• Regulated information with significant penalties for disclosure such as information covered under the Health Information Portability Act or the Internal Revenue Service<br>• Information that is typically exempt from public disclosure |

# Risk Management

## Minimizing risk is an important part of security

# Consequences of not shifting left

- Project Delays and Increased Costs
  - Security deficits cost more when implemented later
- Leaked project information
  - Public perception degraded
  - Integrity of project data
- Non-compliance with regulations and mandates
  - Fines, penalties, rework
- Risks to information systems
  - Breaches – loss of data privacy
  - Malware – system disruption
  - Service attacks – decrease availability

# Resources

- DAS – Cybersecurity Services https://www.oregon.gov/das/OSCIO/Pages/Security.aspx
- ISO 27001 A.6.1.5 Information Security in Project Management
- Cybersecurity & Infrastructure Security Agency (CISA) https://us-cert.cisa.gov/
- Certified Security Project Manager (CSPM) https://www.securityindustry.org/professional-development/cspm-certification/

# Questions