ISSO Cost Modeling and Resourcing

Chrishan Francis Branch Chief
Debbie DeWees, Section Chief
LCDR Travis Coulter, Section Chief

USCG Information Assurance Branch

05/21/2024

History of USCG IA ISSO Cost Modeling

- Six staff members in 2004-2005 for 40 Systems (C&A) – Unsustainable!
- 2008 – 2019 Cost Model started "right-size" the C&A team
  - Cost Model was focused on two goals:
    - What is the # of resources needed for the team
    - How much do we "charge" for the systems
  - Later changed to ISSO vs. C&A team
- 2020-2021 – Onboarding questionnaire created, insourced some ISSO's
- 2024 – working on a contract for USCG

Continue to refine the Cost model on an annual basis

IAB Functions

Assessment & Authorizations

- Authority to Operate (ATO)
  - Document the control implementation language
- Request for Modifications (RFM)

Continuous Monitoring

- POA&M Management
- DoD TASKORD Management (similar to Binding Op Directives)
- Incident Response
- External Audit support (CFO IT Audits, OIG IT Audits)
- DoD Audits – Cyber Operational Readiness Assessment (CORA)
- Cyber health dashboards
- Vulnerability Management

Security Planning (*NEW*)

Steps for Cost Modeling

- Define the ISSO “O&M” function (tasks)
- Capture metrics / LOE for the tasks (informal, or formal)
- Address complexities of systems – This is to get the outliers
    - FIPS Categorization
    - Public facing Y/N
    - Multiple technologies
    - NSS, Privacy, Financial
    - Complex architecture
- Translate the metrics to cost (usually use the 1920HRS annual)
    - Would need to work closely with a Contract for labor rates
- Request a system complete an onboarding questionnaire to understand scope of system
- Each system gets a “voucher” every FY

What we found

- Typically, an ISSO can tackle about 2 or 3 Moderate risk systems
- Not all ISSO's are equal - Skillsets, experience
- For Gov't we look at GS-12 (Jr, Med) and GS-13 (Med, Senior)
  - DoD 8140 Competency Requirements
- Need to stay ahead of acquisition or modernization projects
- Some systems might have a dedicated ISSO depending on complexity

New Challenges

- Modernization of systems while maintaining legacy systems
- Cloud cost modeling
  - Determine # of cloud inheritance controls
  - Refine the cost model to account for IaaS, PaaS, SaaS
- DevSecOps and Software Factory
- Merging/Collapsing of “systems”
  - Assessment of Controls
- Matrix teams/programs and systems
- Reciprocity (for OT, and IS)
- Difficult to recruit and retain workforce
  - Starting to focus on automation
  - Create a baseline standard for ISSO skills (ex: NICE code 722)
  - Going to Career fairs and looking at federal internship programs
- Artificial Intelligence exponential expansion
- Starting to emphasize “Secure by Design”

Questions?