Cybersecurity in the Fast Lane

May 2020

Ryan Christiansen CISSP

412TENG/JT4

DISTRIBUTION STATEMENT A - Approved for public release; distribution is unlimited.
412TW-PA-21214

Scope

- Cybersecurity as it pertains to the System/Software Development Lifecycle
- Cybersecurity is often a cause for delay and a constrain on system design.
  - Unclear requirements
  - Cyber personnel unfamiliar with the system & it's mission
  - Too focused on security
  - Long & often opaque processes for approval

What Does Cybersecurity do?

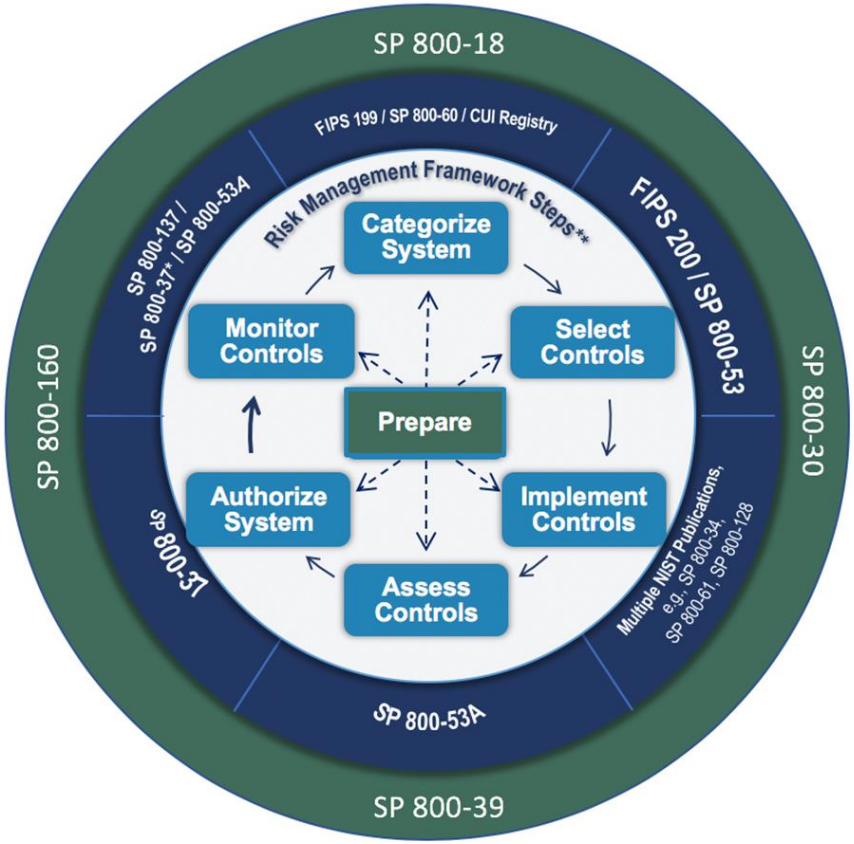
PROCESSES & FUNCTIONS

Cybersecurity Misconceptions

- Exist to shutdown systems
- Have all the requirements needed to be compliant at the requirements stage
  - Have a master list of approved hardware/software

Authorization Process

- NIST's Risk Management Framework (RMF)
  - Steps 0-7
  - Source of many req.
  - Allows flexibility
- Step 2
  - Selecting the requirements for the system/software



Functions of Cybersecurity

- Cybersecurity provides the oversight for system/software development, operations, and maintenance.
  - Secure design
  - Hardware approval authority
  - Software approval authority
  - Ensure compliance
- Can assist in avoiding potholes associated to the myriad of governance and requirements levied by cybersecurity.

Who Should be Involved?

ROLES & RESPONSIBILITIES

Roles

- **Roles within the approval chain of Cybersecurity:**
  - **Program Manager (PM)**
  - **Information System Security Manager (ISSM)**
  - **Information System Security Officer (ISSO)**
  - **System Administrator (SA)**
  - **Users**

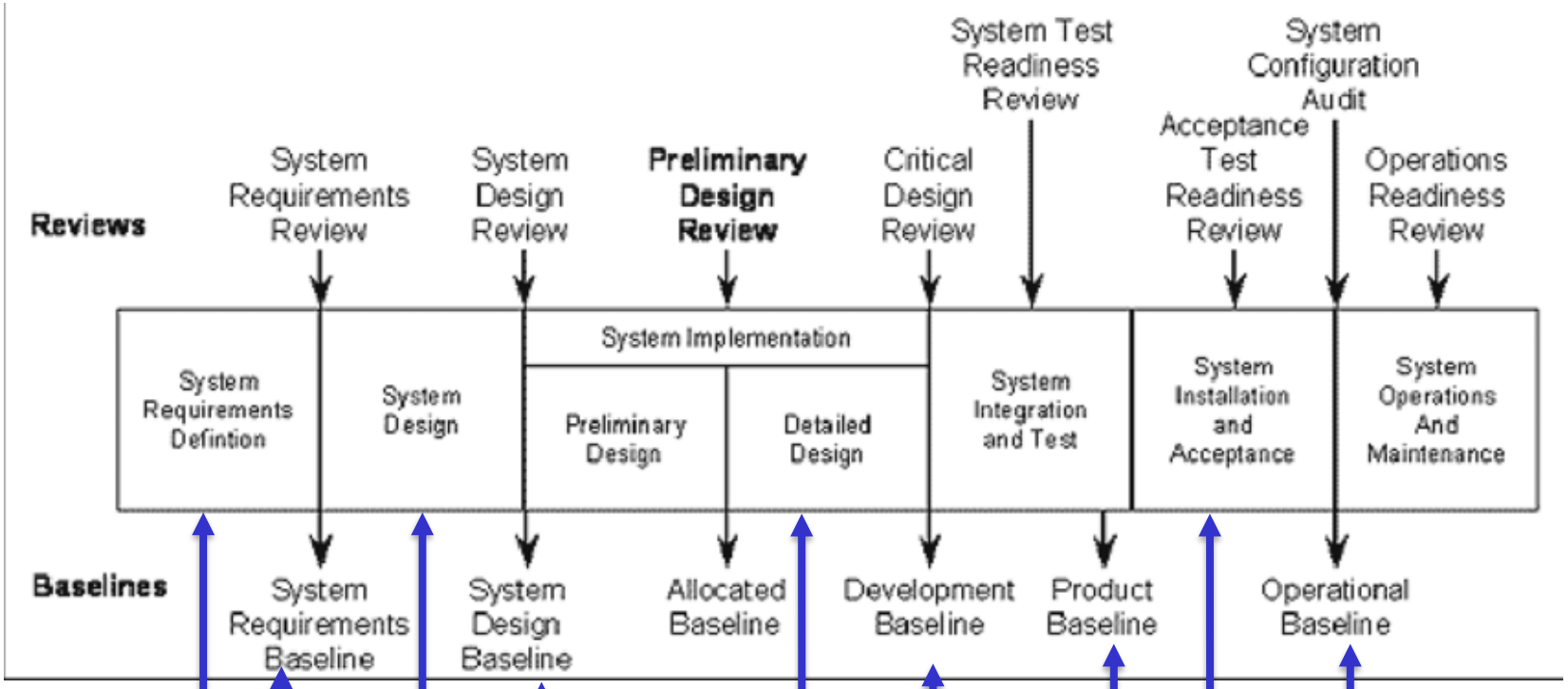
Responsibilities

- PM: ensures that there is a cybersecurity representative during the design meetings.
  - Assists in categorizing the system
  - Ensures requirements are implemented
- Cybersecurity Rep (ISSM/ISSO)
  - Work to categorize system
  - Identify requirements from/for that categorization
  - Assess design choices for compliance
  - Identify approval authorities needed
  - Assess implementation of security controls

When Would They be Involved?

CYBERSECURITY INTEGRATION

The Defense SDLC



"Must do Cybersecurity"

Information type decided, categorization can begin

Categorized

Hardware & Software approval started

Hardware/ Software approval

Needed STIGS identified

Needed STIGS implemented

ATO Submitted

ATO!

What do They Need From Me?

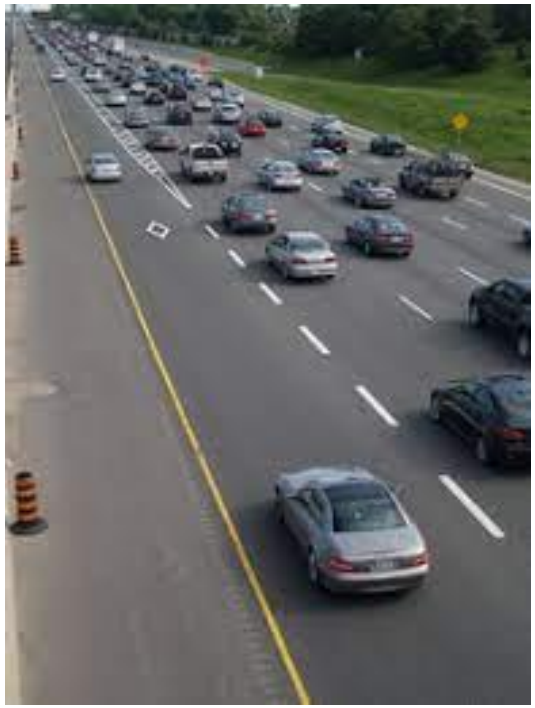
COLLABORATION

What They Need From PMs

- The Program Manager can and should be the "champion" of incorporating someone from the cybersecurity workforce.
- Early involvement to ensure they have intimate knowledge of the system and its mission.
- RMF needs:
  - Step1: Requirements Baseline
  - Step2: System Design Baseline
  - Step3: Development Baseline
  - Step4: During Acceptance Testing
  - Step5: Product Baseline
  - Step6: During Maintenance & Operation

What to do I do Next?

CONCLUSION

Must Work Together

- **The benefits of integrating cybersecurity early and often are:**
  - **Removal of last minute requirements**
  - **Authorization before implementation**
  - **Security tools often improve sustainment and operations**
  - **Design approvals expedited**