JPL's Cyber Security Improvement Project

Scott Morgan, June 27, 2016

Jet Propulsion Laboratory
California Institute of Technology

Cyber Security Landscape at JPL

- Cyber Security Council (CSC)
- Cyber Security Council Management Advisory Group (CSCMAG)
- Cyber Security Improvement Project (CSIP)
- Stakeholder Organizations
  - Engineering and Science Directorate (ESD)
  - Office of the Chief Information Officer (OCIO)
  - Office of Safety and Mission Success (OSMS)
  - Space Asset Protection (SAP)
  - Business Operations Directorate
  - Cyber Defense Engineering Research group
  - Programs/Projects/Missions
- Cyber Defense Laboratory (CDL)
- OCIO Unified Test Lab

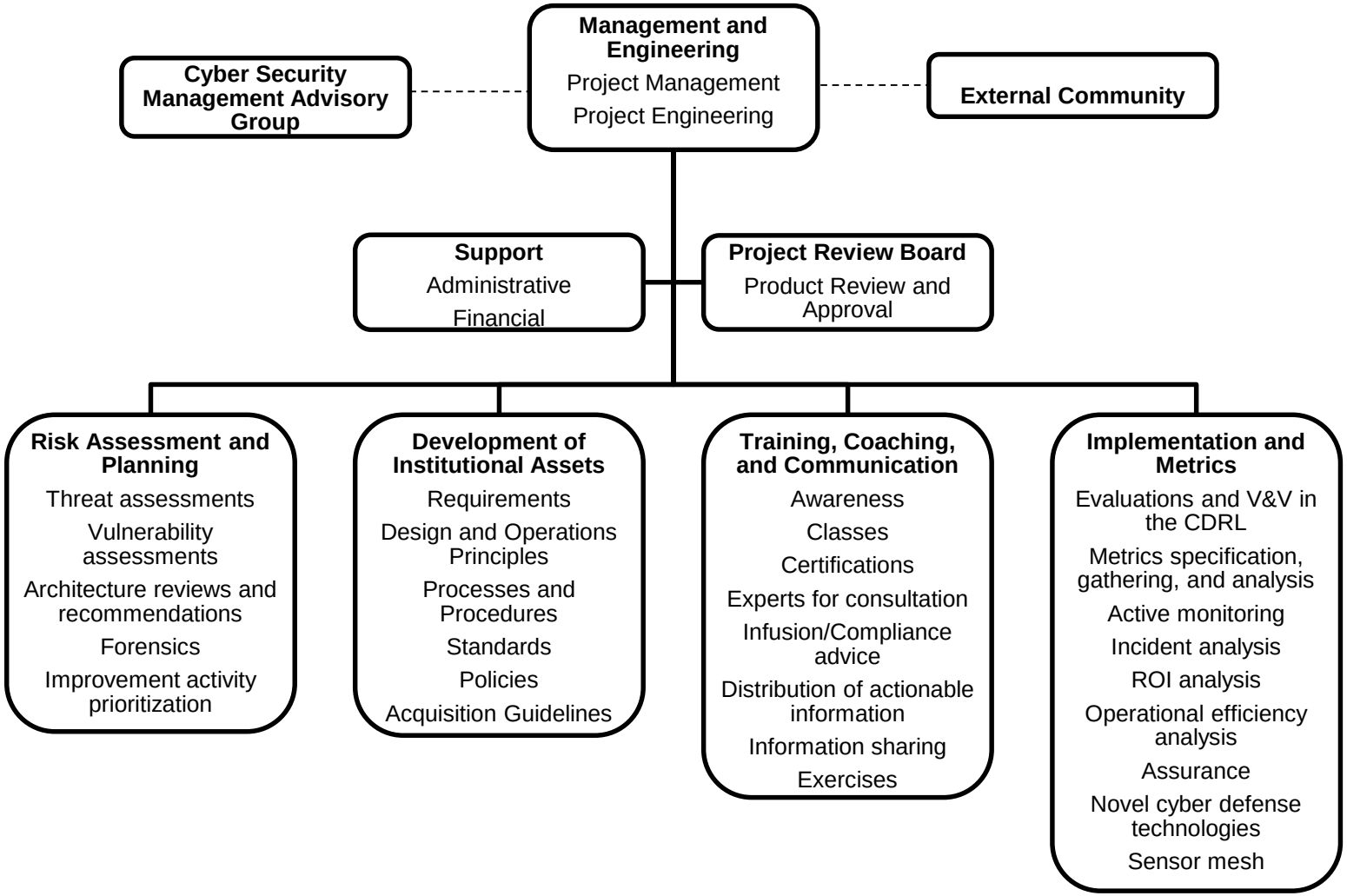
Cyber Security Improvement Approach

- JPL Cyber Security Strategy
  - Tactical and strategic focus
    - Protection of critical assets
      - Top three priorities are related to mission systems
    - Establish sustainable institutional and mission environment that promotes cyber security
  - 21 objectives defined
  - Approved by the JPL Deputy Director and CSC
- CSIP established to achieve these objectives
  - Institutionally funded, multi-year effort
  - Leadership team includes representatives from ESD and OCIO
  - Staff drawn from throughout institution
    - Engineering, CIO, OSMS
    - Supplemented with external subject matter experts
  - Reports to CSC

CSIP Charter

The Cyber Security Improvement Project (CSIP) is an institutionally funded project established to coordinate activities across JPL to meet the goals identified in the JPL Cybersecurity Strategy. The JPL Cybersecurity Strategy applies to the development and operation of assets supporting missions, providing multi-mission support, conducting business operations, and the underlying institutional infrastructure. CSIP will work with ESD, OCIO, and OSMS to integrate existing and planned activities with new CSIP-sponsored initiatives to fully address the goals and objectives of the Strategy.

CSIP Functional Organization



Near Term Activities

- Established a framework to organize activities, track progress (NIST 800-53 based)
- Identification and tracking of critical assets
- Sensor mesh design and development
- SW supply chain monitoring
- SwDLC improvements
- Develop approach to cyber risk assessment
- Benchmarking
- Establish partnering relationships
- Initiate communication/education/training activities for the JPL community
- Vulnerability Assessments - CDL

Current Pilot Efforts

- Establish the evaluation process for intrusion sensors aimed at mission system deployment
- Establish cyber-focused test processes for incorporation into the life cycle of mission systems
- Credentialed Scanning
- CodeSonar Static Code Analysis Tool
- Automated Asset Inventory Collection
- Evaluation of tools for vulnerability identification
- Training: Ethical Hacking
- CCARAT: Model-based cyber security risk assessment tool

Challenges

- Risks are managed at the project/mission level
  - Lack of a broad perspective on cyber risk encompassing both institutional and mission environments
- Cyber security threats to JPL are not fully recognized
- Balancing security and usability
- Knowledgeable project staff
- Compliance verification and monitoring
- Traditional project maintenance life-cycle vs. need to respond to a dynamic threat environment

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov

Copyright 2016 California Institute of Technology.
U.S. Government sponsorship acknowledged.