NAWCAD Lakehurst ALRE Department

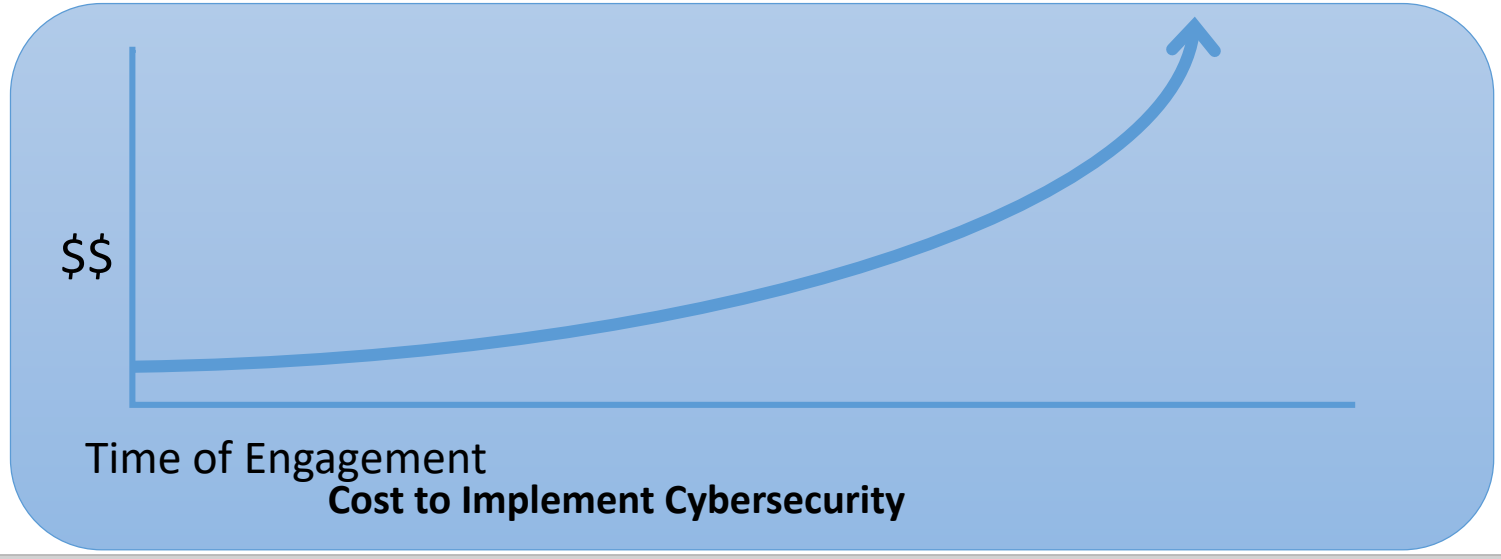
23 July 2020

Presented to: SBR Event

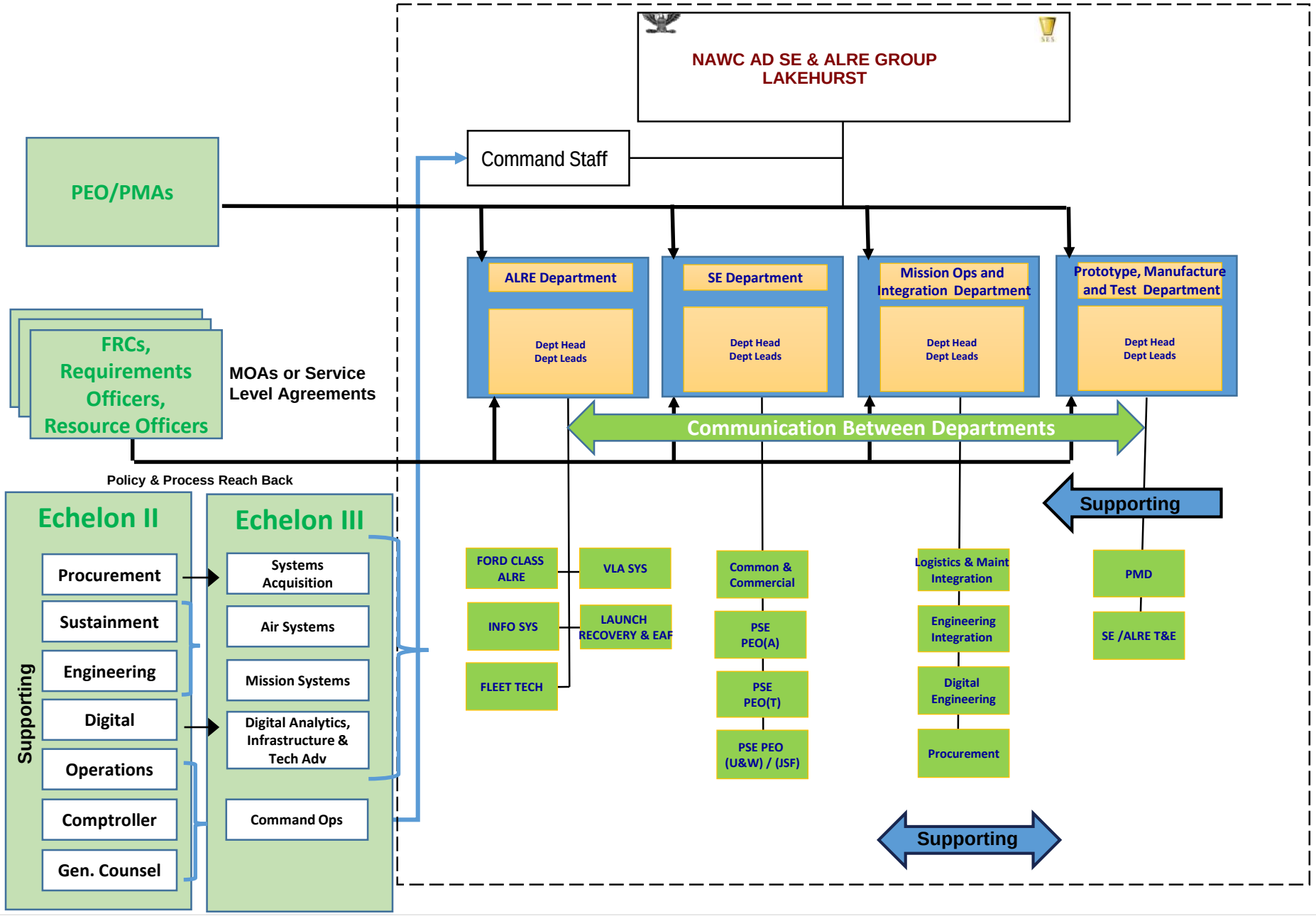
Presented By: Gail Edwards, ALRE Department Cybersecurity Lead; gail.edwards@navy.mil

Overarching Vision

- The goal of cybersecurity is to secure systems and reduce the Navy's overall threat exposure
  - Obtaining an accreditation (ATOs and IATTs) is a validation of this process; however, ATOs are not the ultimate end-goal
- Cybersecurity engagement must occur early in development
  - Significantly reduces the lifecycle costs of producing a secure system



Cybersecurity is not just about being compliant with policy; it's about securing the tools and assets the warfighter relies on every day

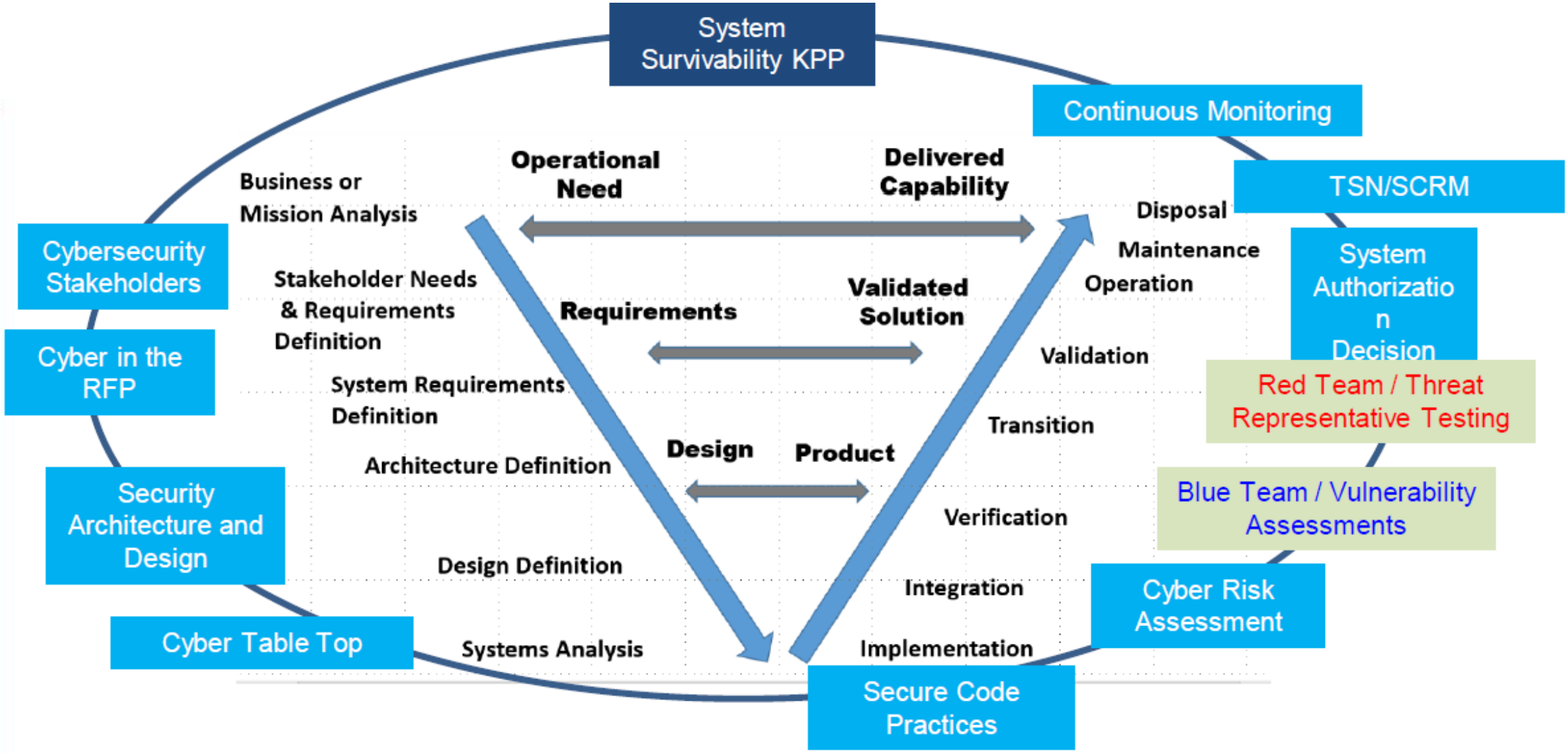

NAWC AD SE & ALRE GROUP
LAKEHURST
Command Staff
PEO/PMAs
FRCs, Requirements Officers, Resource Officers
MOAs or Service Level Agreements
ALRE Department
Dept Head
Dept Leads
SE Department
Dept Head
Dept Leads
Mission Ops and Integration Department
Dept Head
Dept Leads
Prototype, Manufacture and Test Department
Dept Head
Dept Leads
Communication Between Departments
Policy & Process Reach Back
Supporting
Echelon II
Procurement
Sustainment
Engineering
Digital
Operations
Comptroller
Gen. Counsel
Supporting
Echelon III
Systems Acquisition
Air Systems
Mission Systems
Digital Analytics, Infrastructure & Tech Adv
Command Ops
FORD CLASS ALRE
INFO SYS
FLEET TECH
VLA SYS
LAUNCH RECOVERY & EAF
Common & Commercial
PSE PEO(A)
PSE PEO(T)
PSE PEO (U&W) / (JSF)
Logistics & Maint Integration
Engineering Integration
Digital Engineering
Procurement
PMD
SE /ALRE T&E
Supporting

ALRE Cyber Mission

- Responsible for providing Cybersecurity engineering support to ALRE POR's and RDT&E Labs
  - Ensures Cyber requirements are designed, tested and optimized within the systems engineering construct for all ALRE development and/or acquisition products
  - Maintains awareness of current cybersecurity threats and shares the resulting implications to supported systems
  - Integrated within the software development teams to ensure software assurance practices are followed
  - Oversee Risk Management Framework (RMF) process, ensuring systems obtain an accreditation
    - Risks are a function of threat/vulnerability/impact
- Provide qualified and certified cybersecurity workforce professionals to serve as Cybersecurity Engineers on various ALRE System
  - Oversee ALRE specific cybersecurity specialties within the Digital Division with the Mission Ops and Integration Department including:

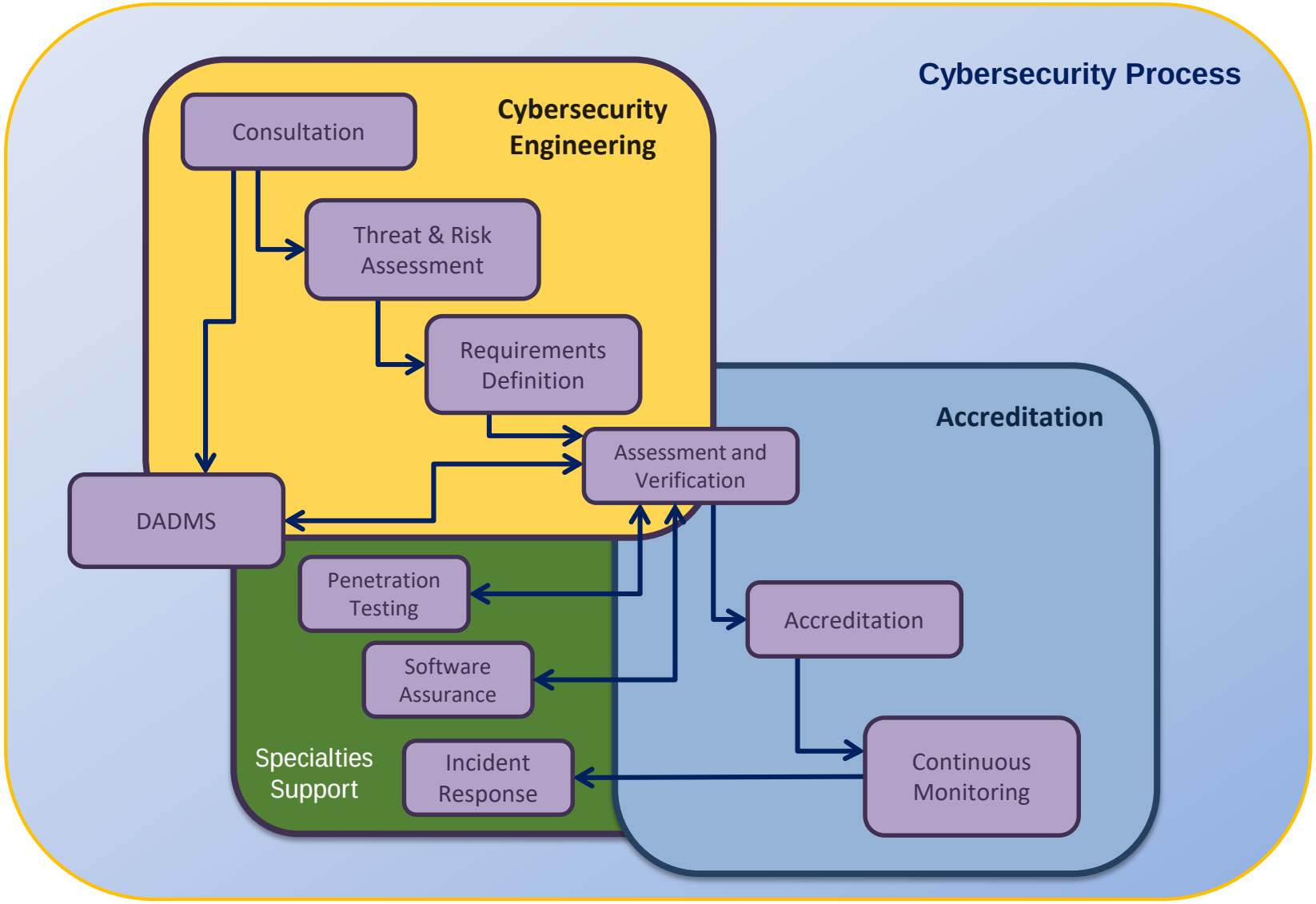
    - Federated Penetration Testing
    - Cyber Risk Assessment
    - Risk Management Framework
    - Threat Intel
    - Incident Response and Forensics
    - Cross Domain Solutions
    - Supply Chain Risk Management

ALRE Cybersecurity Engineering

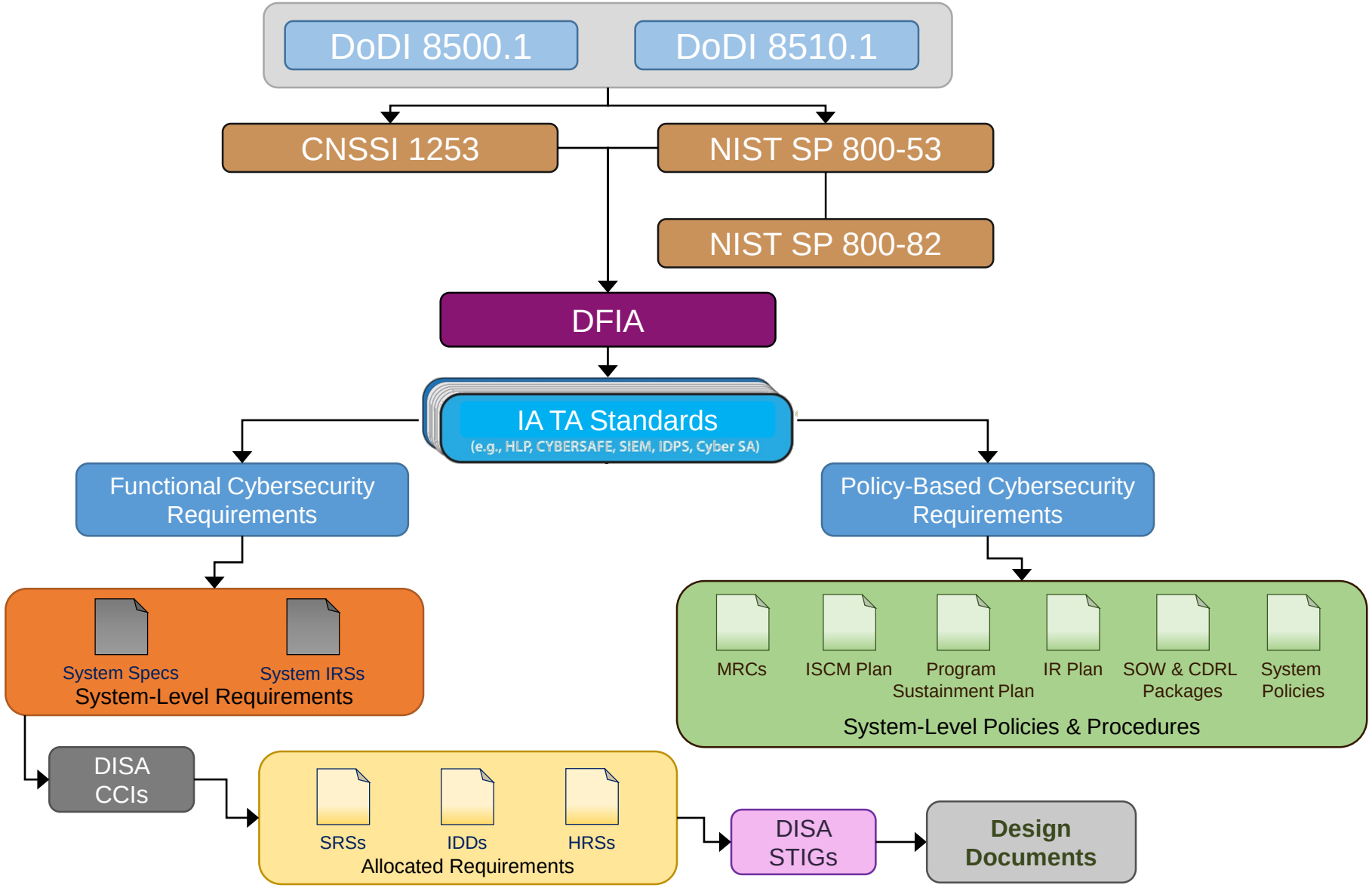


Ref: ISO/IEC/IEEE 15288, Systems and Software Engineering- System Lifecycle Processes, 15 May 15

Cybersecurity Processes



Requirements Traceability



Opportunities for SBR

- Augment the ALRE government team
  - Cybersecurity Engineering –requirements definition based on NIST 800-53 are understood and implemented
  - Solutions Architect/Computer Network Architect- implementation of DIFIA architect for mission systems; definition and design
  - Secure Development – Secure coding expertise utilizing secure container environment (MySQL, GitOps, RedHat) with an Agile process (DEVSECOPS), software assurance tools, etc.; government goal is to perform quality secure code, continuous integration, continuous delivery pipeline with continuous authority to operate