Delivering Monthly Cyber Security Updates with Agile

SEAWATCH
U.S. COAST GUARD

Mission Ready, Mission Essential

What is SeaWatch?

SeaWatch is an enhanced Coast Guard C2 system that integrates navigation and tactical sensors, communications, and optical surveillance systems to provide superior situational awareness of the operational environment.

Delivering Capability & Commonality

Navigation

Modular Apps

Radar

SeaWatch Core

Modular Hardware & Sensors

COP

Information Assurance
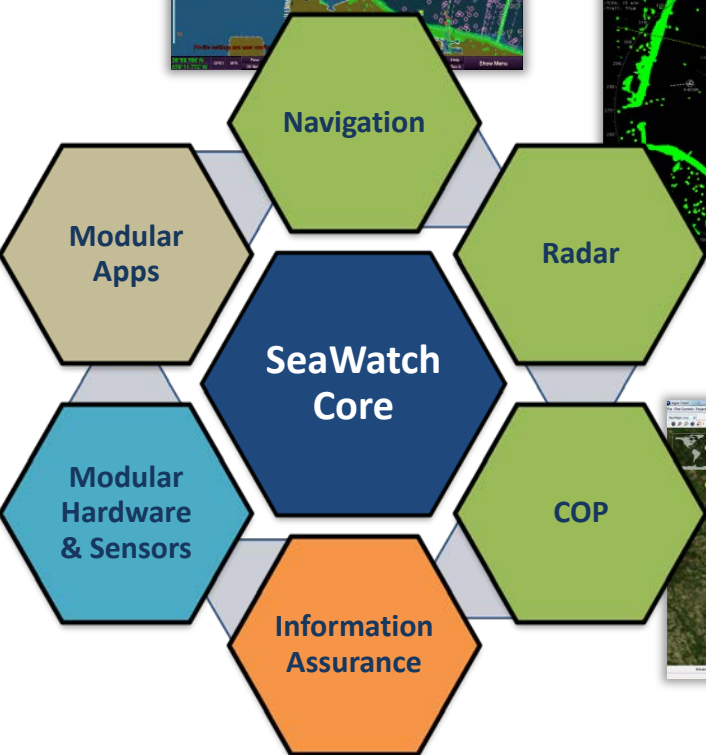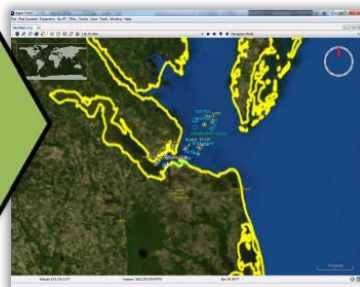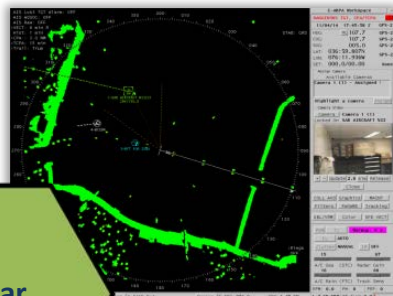
Developed and Sustained using Agile Software Development Methods at C3CEN

SeaWatch Core scales to cutter requirements
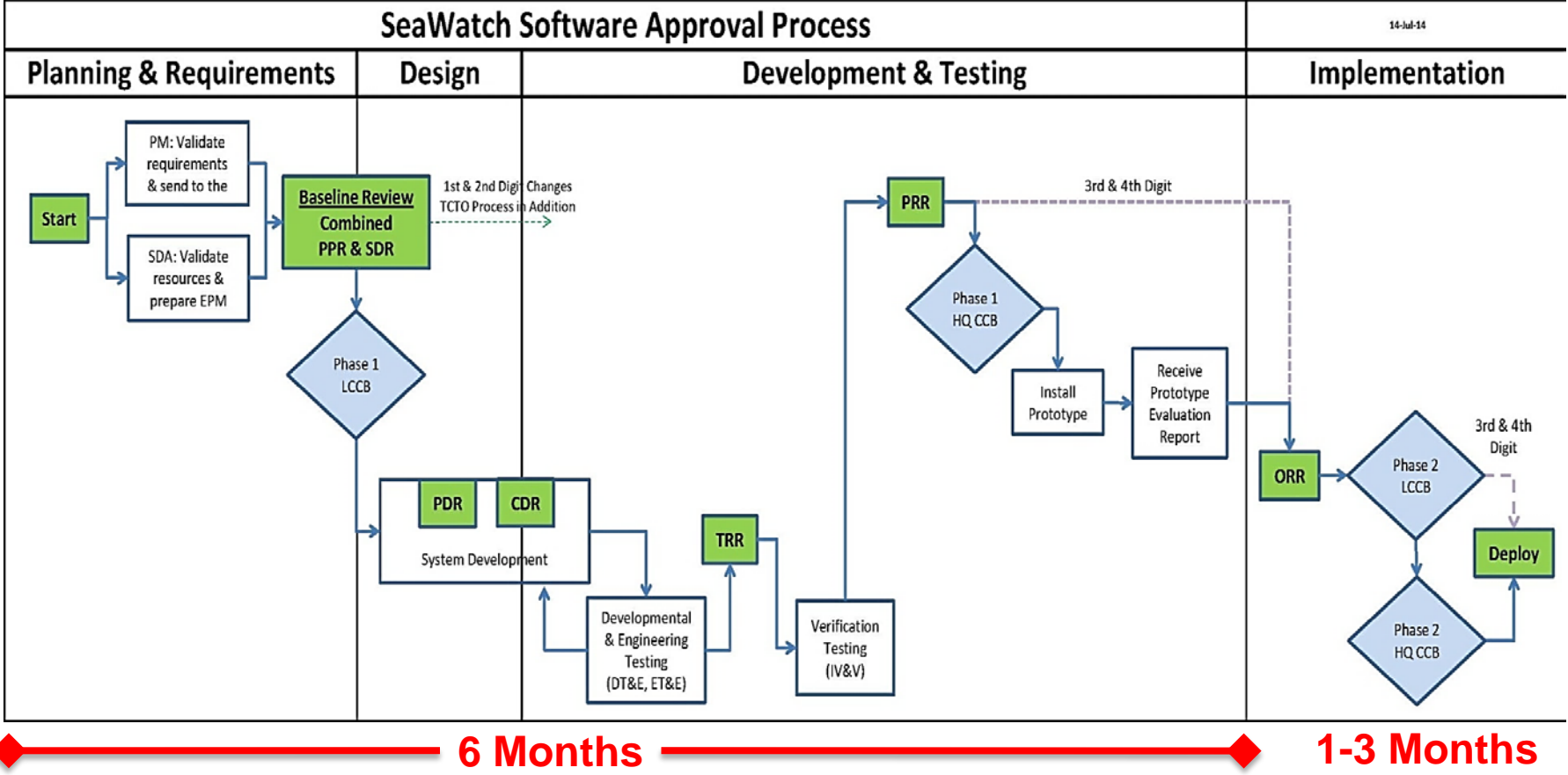

WHEC

WMEC

FRC

WPB

OPC & PIB

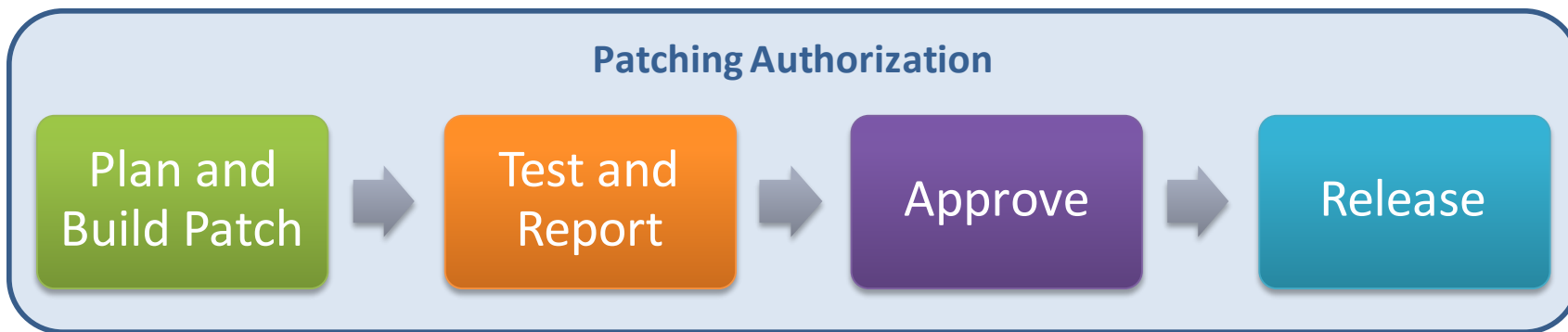WLB & IB

Original Development Process
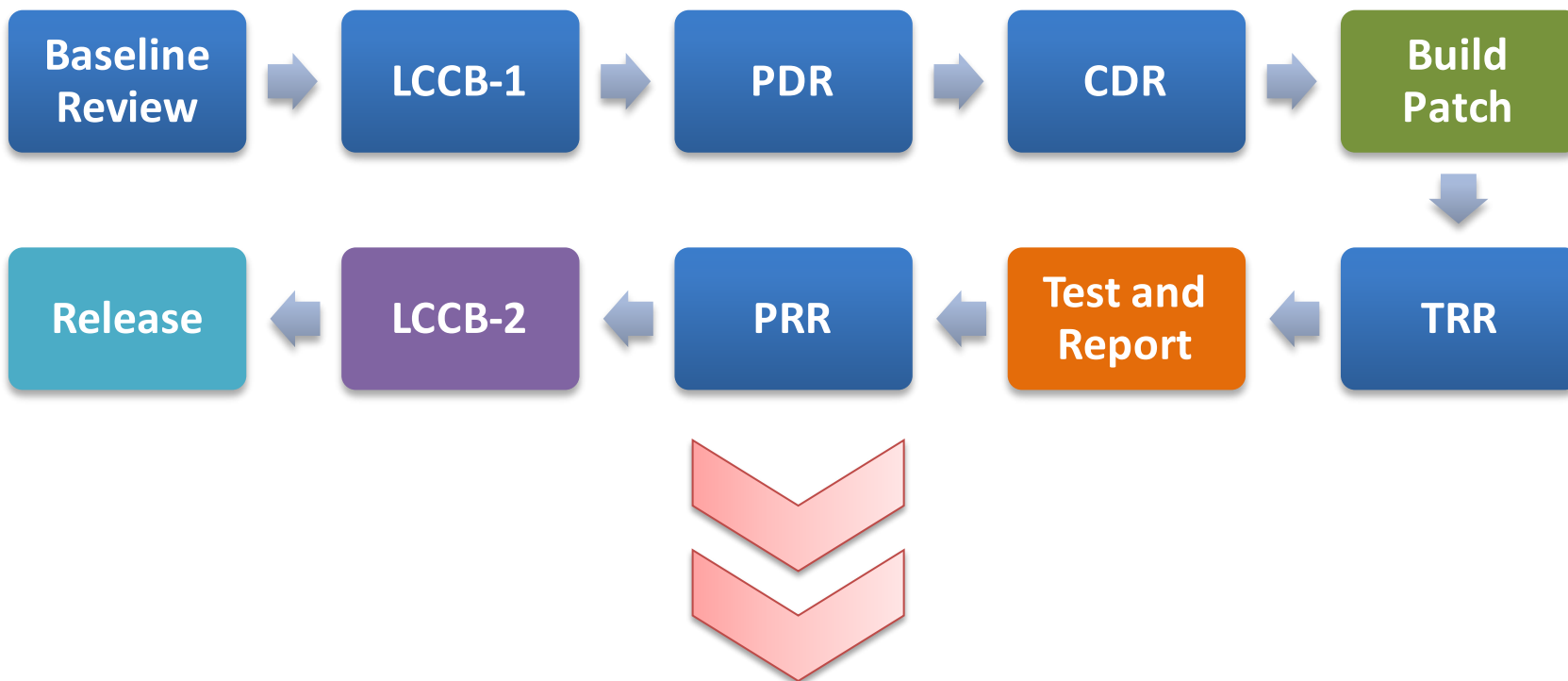
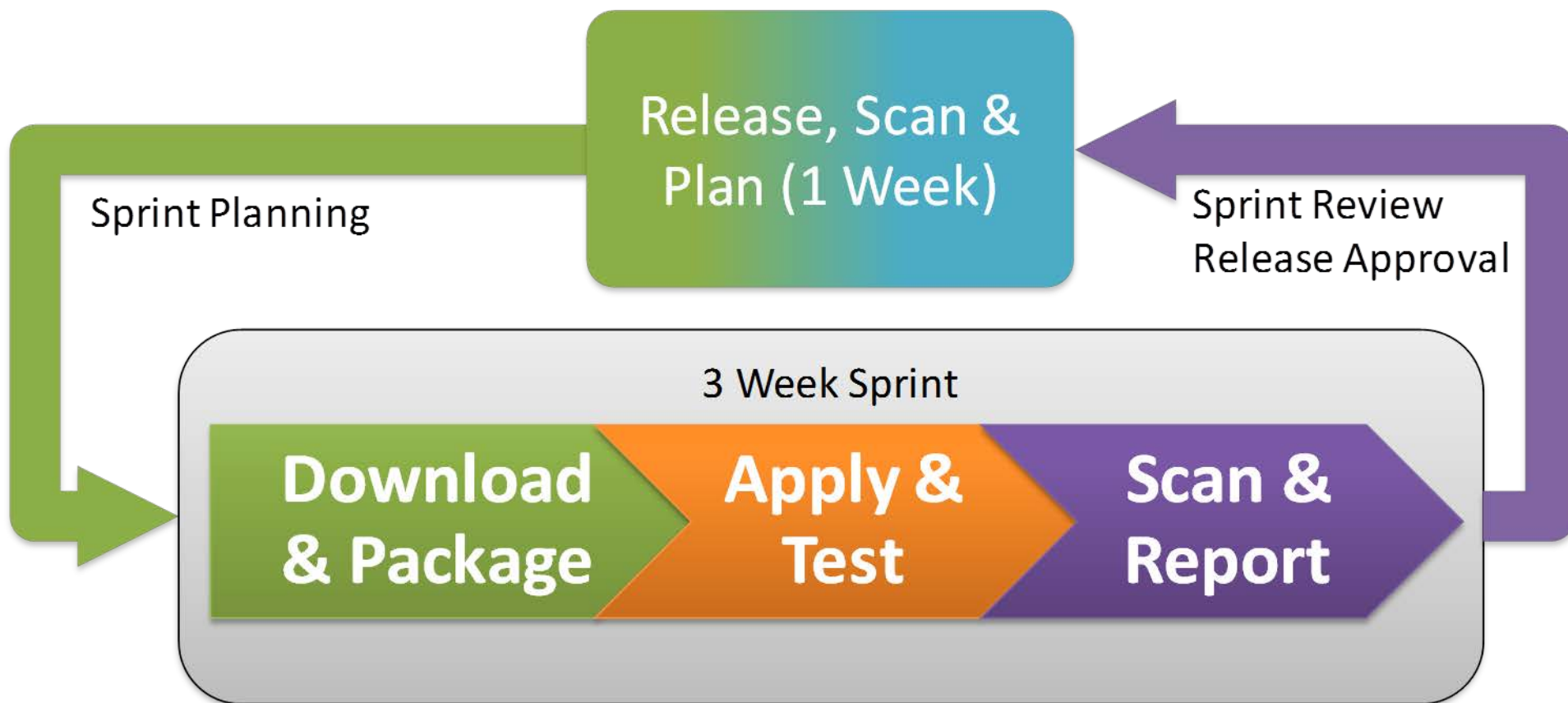| Increment	Significance
1st Digit	Architectural change
2nd Digit	Addition of new capability
3rd Digit	Resolve STRs & SIRs; Application Updates
4th Digit	Security update & critical config change

6 Months — **1-3 Months**

Streamline the Process

Baseline Review → LCCB-1 → PDR → CDR → Build Patch

↓

TRR → Test and Report → PRR → LCCB-2 → Release

Patching Authorization

Plan and Build Patch → Test and Report → Approve → Release

Ground rule: 4th digit patch can not impact functionality

Agile Information Assurance

Release, Scan & Plan (1 Week)

Sprint Planning

Sprint Review Release Approval

3 Week Sprint

Download & Package → **Apply & Test** → **Scan & Report**

1 Month

Release Process

Approval Memo

Pre/Post Scan Results

Release Message

Upload Patch to Cloud Storage

Automatic Install

Reporting

Retrospective

- Successfully released 12 patches (Dec 2015 – Dec 2016)
- Installation has lagged behind releases
    - Cutter operational schedule impacts installation rate
    - Automated installation reporting is a critical tool
- Patch tool iteration
    - Every two sprints we prioritized installation efficiency
    - Started with manually running installer on every computer
    - Merged into one fully automatic installer; <u>reduced workload by 90%</u>
- Cyber security overhead has grown 2x in a year!
    - Started with 20 findings per month, on average
    - Recently averaging 40+ findings per month
    - IAVA and Cyber TASKORDs add additional requirements

- Transition to remote deployment and installation
  - SCCM or Distributed File Services
  - Utilize background install and notification for restart

- Analyze process for further efficiencies
  - Streamline IAVA and TASKORD compliance reporting
  - Utilize built-in ACAS tracking mechanisms
  - Further streamline approval process

Questions?