

2016 Defense Health Information Technology Symposium

Cybersecurity Requirements for Medical Device Acquisition



“Medically Ready Force...Ready Medical Force”

“A joint, integrated, premier system of health, supporting those who serve in the defense of our country.”



“Medically Ready Force...Ready Medical Force”

Learning Objectives

- Discuss the cybersecurity challenges involving the medical device/equipment acquisition process
- Describe NDAA 2016, section 2368 and the features of the CRADA to investigate process improvements (research goals)
- Explain roles and responsibilities of each partner in the CRADA
- Recognize the output of the CAP CRADA for USAMMA and Industry

Agenda

- Medical Device Acquisition Problem Statement
- Cooperative Research and Development Agreement (CRADA) Background
- US Army Medical Materiel Agency (USAMMA) Cybersecurity Assessment and Pre-Authorization (CAP) CRADA
- Roles and Responsibility
- CAP CRADA Process
- Summary

Medical Device Acquisition Problem Statement

- USAMMA / DoD:
 - Difficulty in achieving cybersecurity standards in a timely manner during acquisition process
 - Security over capability:
 - Equipment not procured due to security risks/certification uncertainty
 - Limited pool of medical devices – manufacturers unwilling or unable to meet security requirements
 - Exacerbating Environment – More stringent cybersecurity policies and plan to shift more responsibility and risk to industry partners

Develop a Cybersecurity Pre-Assessment Process/Mechanism

Medical Device Acquisition Problem Statement

- Manufacturer Industry:
 - ‘Chicken and Egg’ cybersecurity quandary: They won’t buy unless you have “it”, you can’t get “it” until they buy
 - Current procurement process offers limited window to comply with requirements
 - No formal sponsorship/guidance outside the procurement process
 - Security engineering currently an additive “bolt-on” vs a built-in “baked-in” process
 - Medical device/equipment industry is not as flexible as the IT industry
 - FDA and patient safety requirements limits reengineering timeliness and ability
 - Longer lead time to meet cybersecurity standards
 - Non-sponsored cybersecurity compliance initiatives are riskier
 - Cybersecurity process variances amongst DoD services/agencies
 - Not all DoD required controls/tools are accessible to the public (PKI protected)
 - Over engineer/under-engineer

Develop a Cybersecurity Pre-Assessment Process/Mechanism

“Medically Ready Force...Ready Medical Force”

Cooperative Research And Development Agreement (CRADA) Background

- NDAA 2016, section 2368:
 - (2) “..reengineer management and business processes and adopt best-business and personnel practices...in connection with the capability of the Centers”
 - (3) “..may conduct one or more pilot programs...to test any practices referred in paragraph (2)”
- A written agreement between one or more federal laboratories and one or more non-federal parties under which the government, through its laboratories, provides personnel, facilities, equipment or other resources with or without reimbursement (but not funds to non-federal parties).
- The non-federal parties provide personnel, funds, services, facilities, equipment or other resources to conduct specific research or development efforts that are consistent with the mission of the laboratory.
- CRADAs are authorized by 15 U.S.C. 3710a. The governing regulation is AR 70-57, Military-Civilian Technology Transfer, dated 26 February 2004.
- Benefit: Creating new products, **processes**, and intellectual property applicable to mission and commercial goals

USAMMA CAP CRADA Research Proposal



2016 Defense Health Information Technology Symposium

- Establish a government sponsored/endorsed cybersecurity pre-authorization activity outside procurement process to benefit government (USAMMA) and industry (medical equipment manufacturer/supplier vendors)
- Establish the Cybersecurity Assessment and Pre-Authorization (CAP) CRADA research study
- USAMMA will provide sponsorship* to better prepare industry to receive authorization (ATO) outside of formal acquisition process
 - Limited laboratory capability will be available at USAMMA
 - Provides ability for industry to conduct cybersecurity testing at non-government site for complex equipment or if mutually beneficial to government and industry

*CAP CRADA sponsorship does not grant ATO but will help assess manufacturer's likelihood of success

USAMMA CAP CRADA

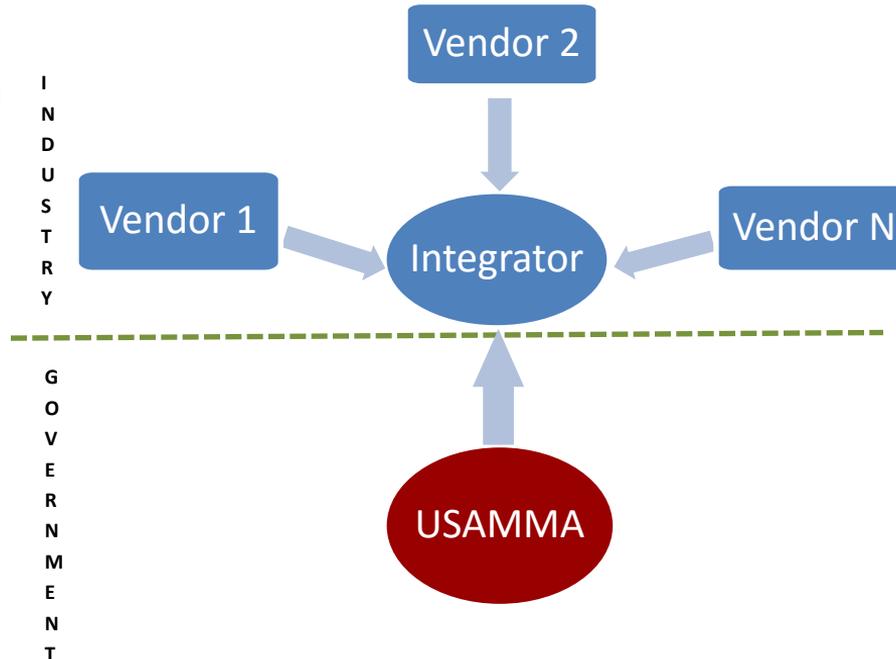
Predicted Outcomes

- Reduced time between procurement phase to operational use phase
- Improve industry's compliance to DoD cybersecurity requirements:
 - Reduction of re-work/re-engineering
 - Improved ability to compete and complete an acquisition process
 - Deliver operational product to government faster
 - Improved security by having mechanism to 'bake-in' security requirements
 - Improve marketability of products by having pre-authorization certification for acquisition consideration
- Increased product availability to meet DoD needs
 - Improved USAMMA purchasing power
 - Increased medical device product availability and options
 - Increased DoD cybersecurity posture

CAP CRADA offers potential significant benefits to both DoD and Industry

USAMMA CAP CRADA Relationship Structure

USAMMA establishes
single relationship with
integrator partner
(managing the vendor
partners)



Features:

- Single CRADA agreement (pass down process)
- Independent industry integrator partner
- Promotes Best Practices
- Scalable (shift workload to integrator partner)

“Medically Ready Force...Ready Medical Force”

USAMMA CAP CRADA Management Structure



2016 Defense Health Information Technology Symposium

- CRADA Sponsor
 - Commander, United States Army Medical Materiel Agency (USAMMA)
- Government principal investigator (PI)
 - Product Manager (PdM), Cybersecurity, MAJ Jon Deeter
- CRADA Management
 - George Cook, Office Research Technology Applications (ORTA)
- CRADA legal support
 - Mr. Robert Charles, JD, Chief, Medical Research Law

“Medically Ready Force...Ready Medical Force”

Roles and Responsibilities: USAMMA



2016 Defense Health Information Technology Symposium

- Federal Lab CRADA sponsor and manager
- CRADA Enrollment Authority Decision
- Regulatory authority on the cybersecurity process
- Manages government resources and project task obligations
- Cybersecurity pre-authorization determination authority

“Medically Ready Force...Ready Medical Force”

Roles and Responsibilities: DeltaStrac, LLC (Integrator)



Defense Health Agency

2016 Defense Health Information Technology Symposium

- Approved unbiased CRADA Industry Integrator
- Industry partner principal investigator (PI)
- Jointly develops the application and enrollment acceptance process
- Researches and manages the recruitment and nomination of industry partners
- Provides and coordinates industry personnel, tools and facilities to support CRADA requirements
- Manages industry project task obligations
- Provides CRADA management and technical services

“Medically Ready Force...Ready Medical Force”

Roles and Responsibilities: Industry Partner



2016 Defense Health Information Technology Symposium

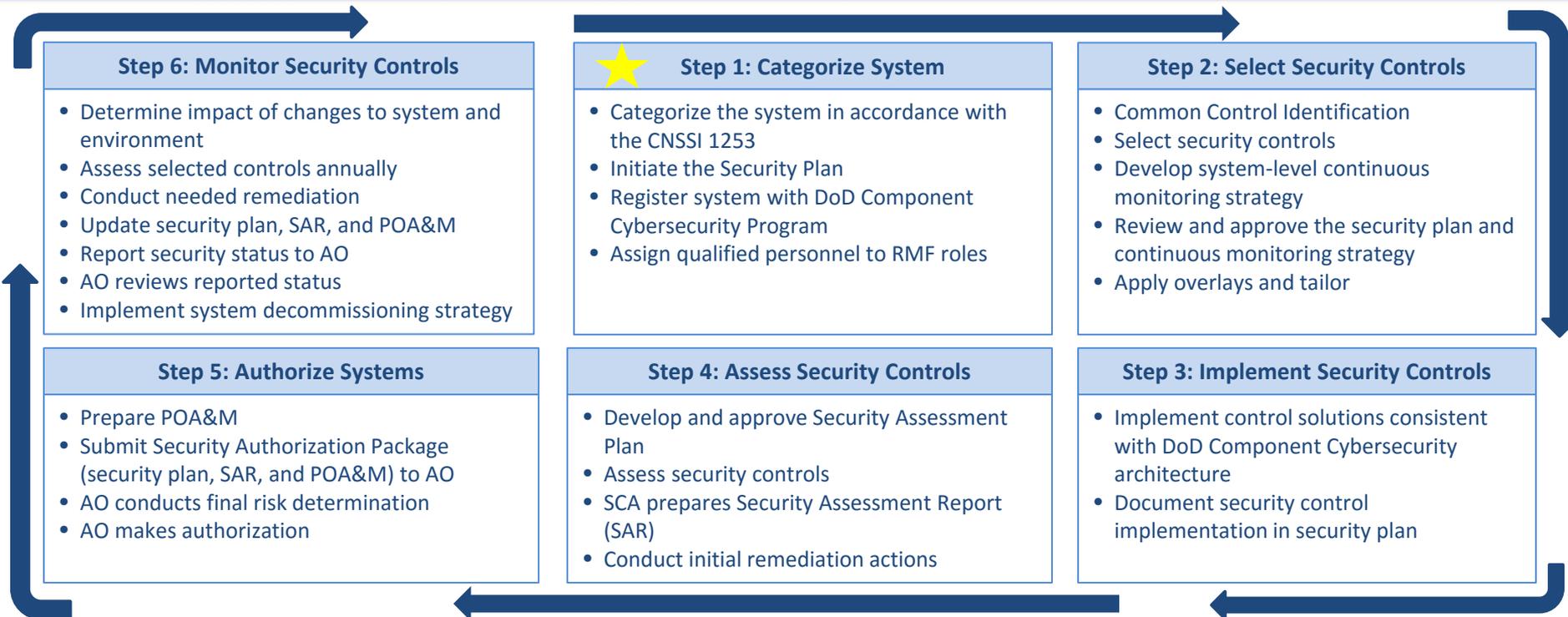
- Vendor participant is a manufacturer, developer or seller of medical device to DoD
- Conform to USAMMA CRADA agreement
- Establish support services contract with DeltaStrac
- Provide industry resources and facility requirements
- Provides technical and administrative information and support related to medical device

“Medically Ready Force...Ready Medical Force”

DoD Risk Management Framework (RMF)



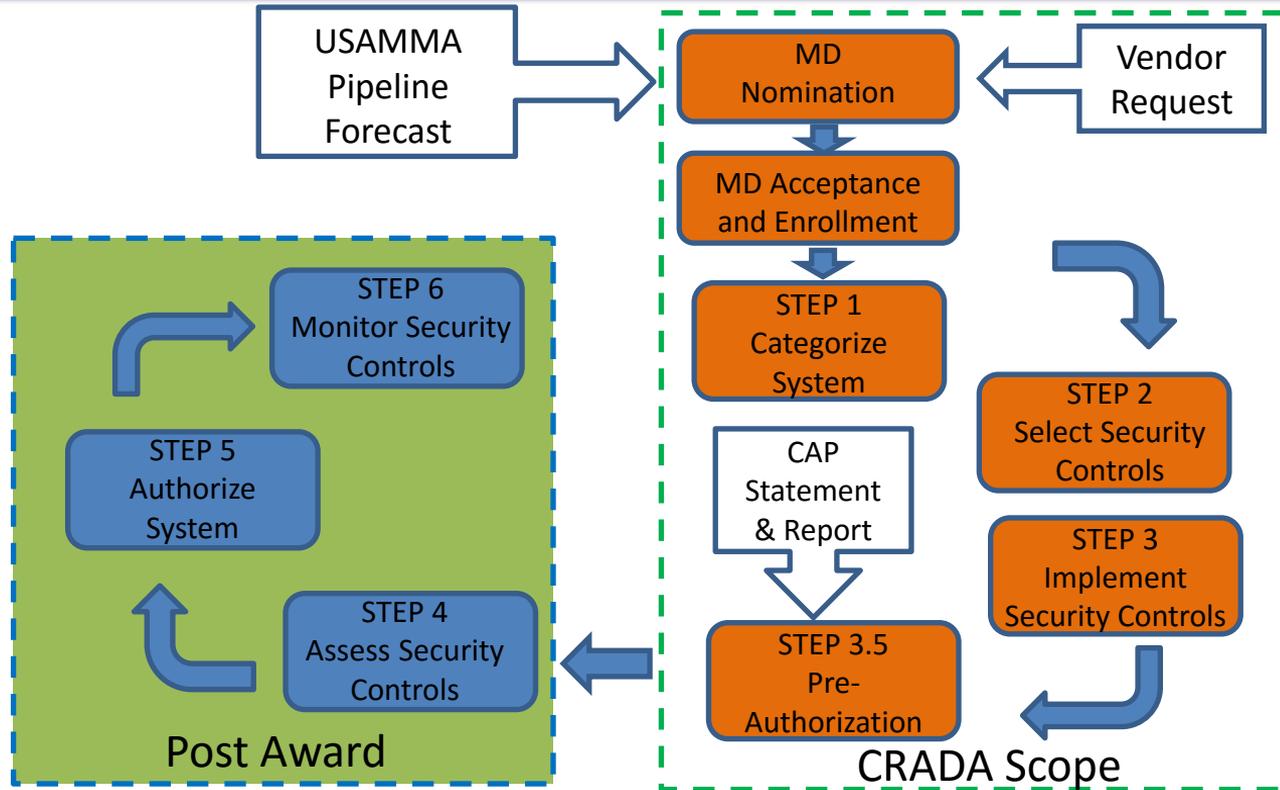
2016 Defense Health Information Technology Symposium



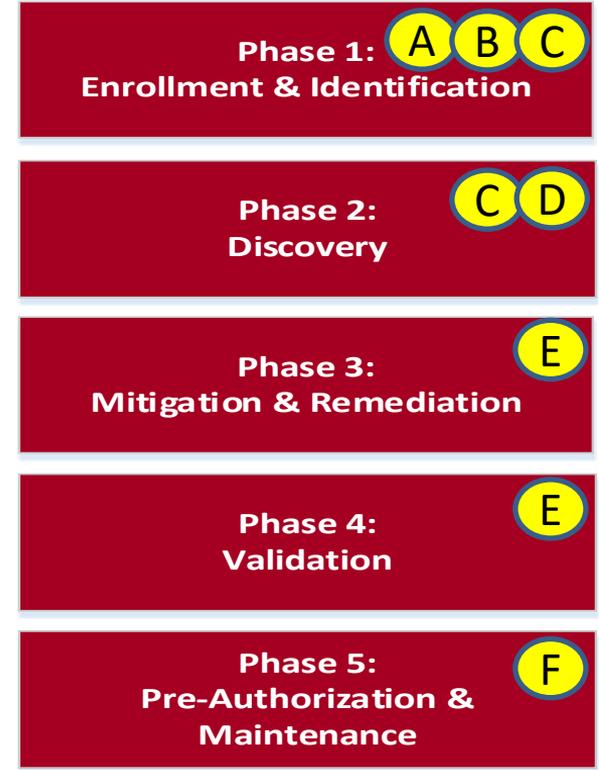
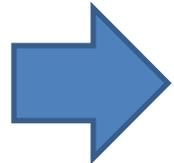
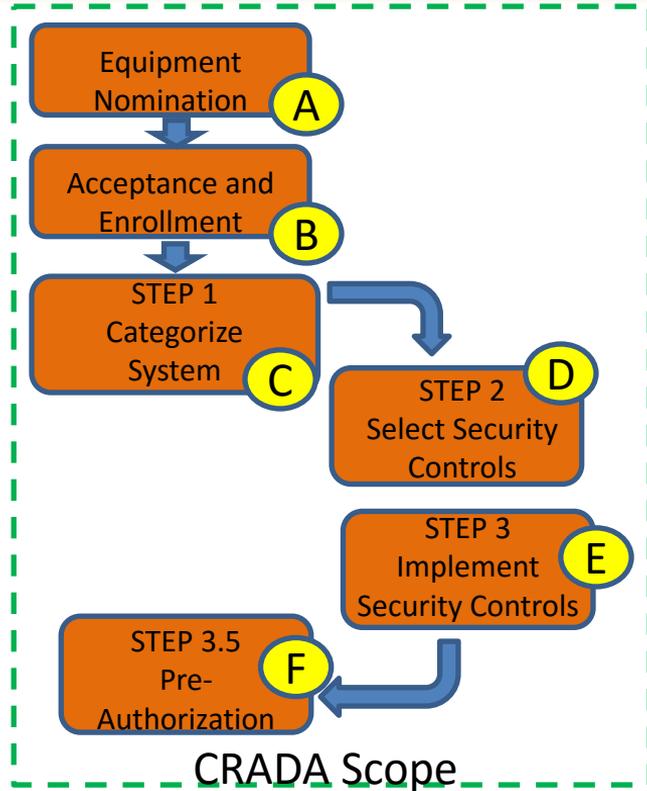
Current State: All Steps are Post Procurement/ Acquisition Activities

“Medically Ready Force...Ready Medical Force”

CAP CRADA Process Scope

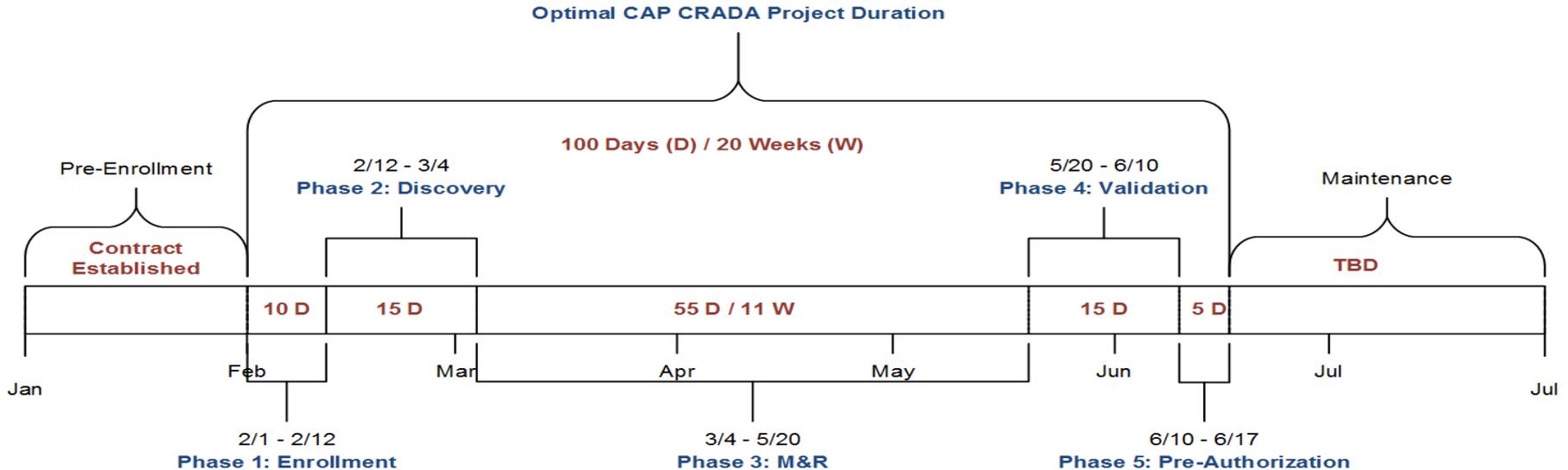


CAP CRADA Process Phases



“Medically Ready Force...Ready Medical Force”

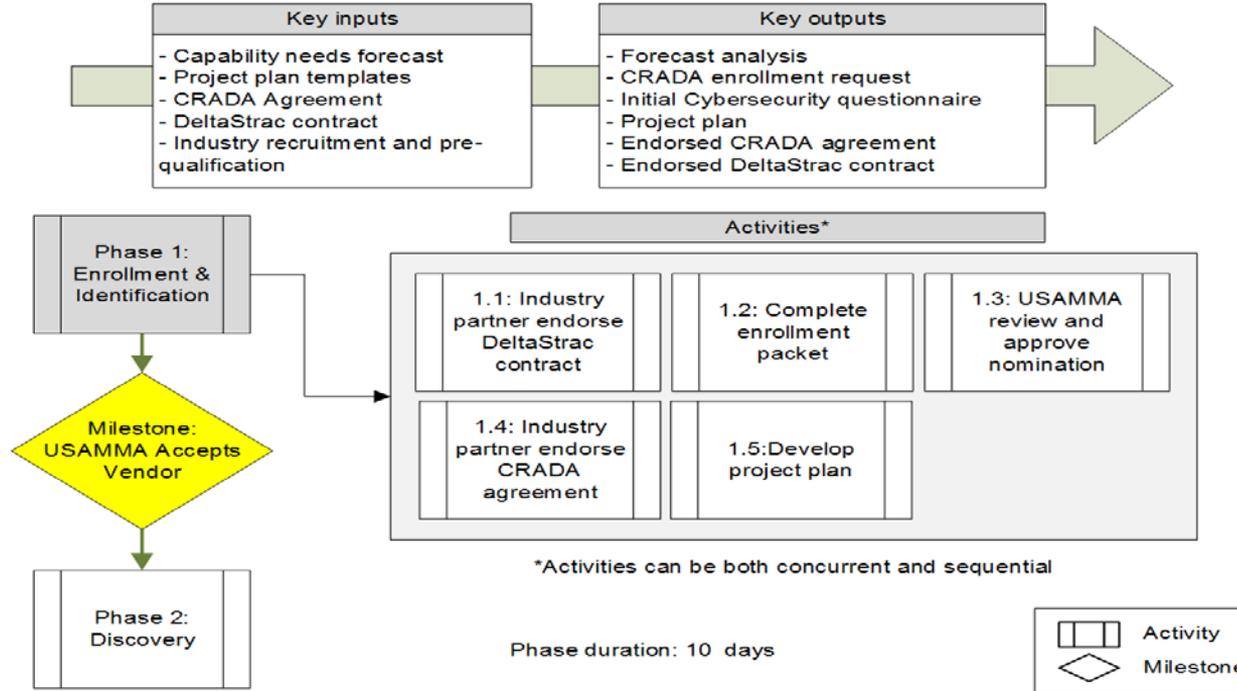
CAP CRADA Optimal Project Timeline



- Start to Finish representative timeline
- Multiple projects will introduce lags between Phase 1 and Phase 2

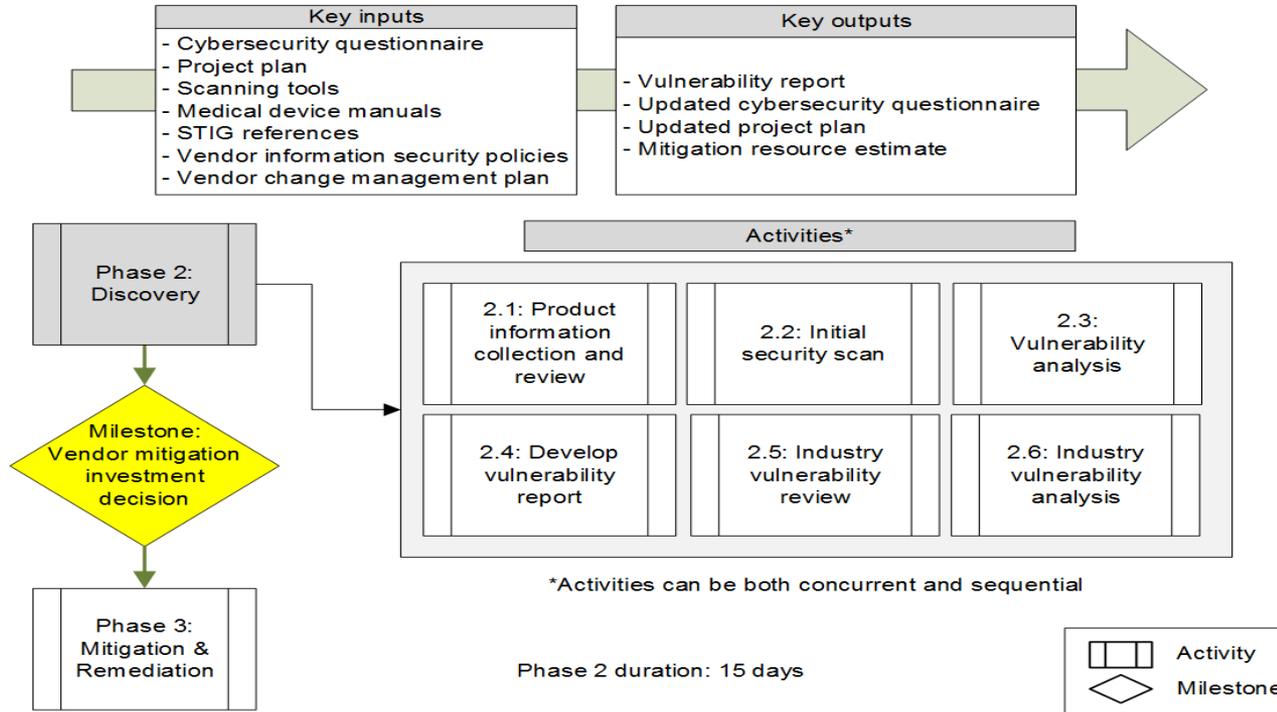
“Medically Ready Force...Ready Medical Force”

Phase 1: Nomination & Enrollment



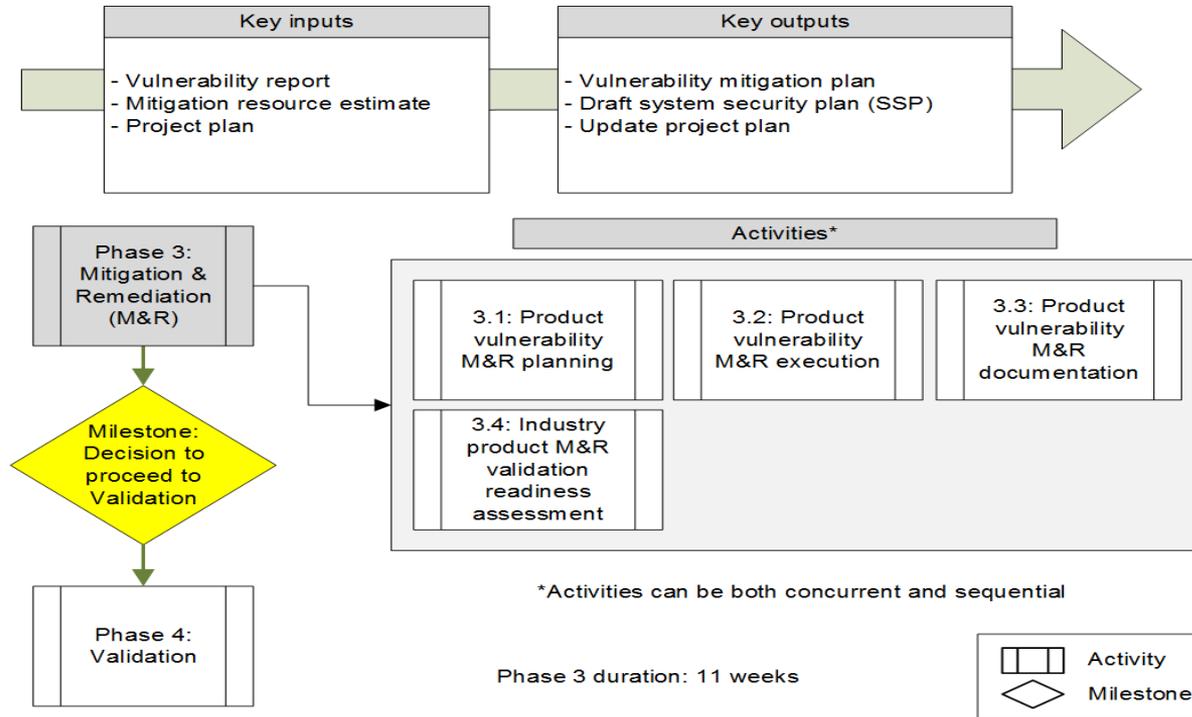
“Medically Ready Force...Ready Medical Force”

Phase 2: Discovery



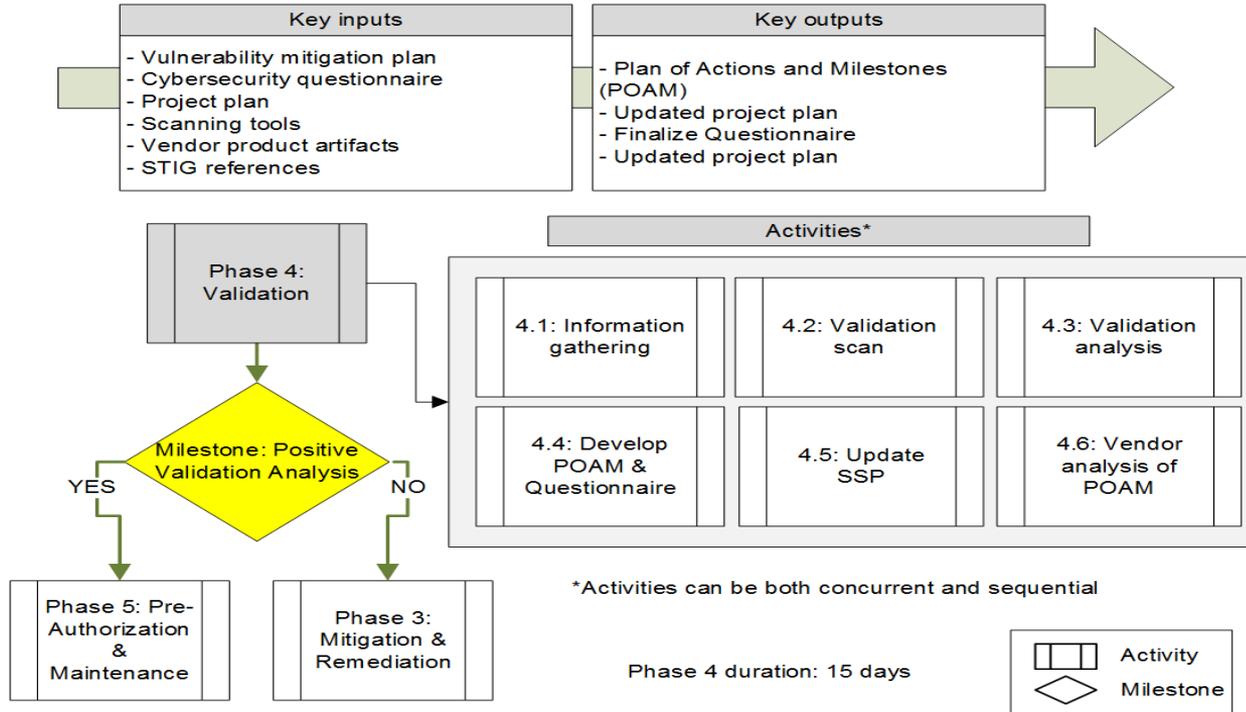
“Medically Ready Force...Ready Medical Force”

Phase 3: Mitigation & Remediation



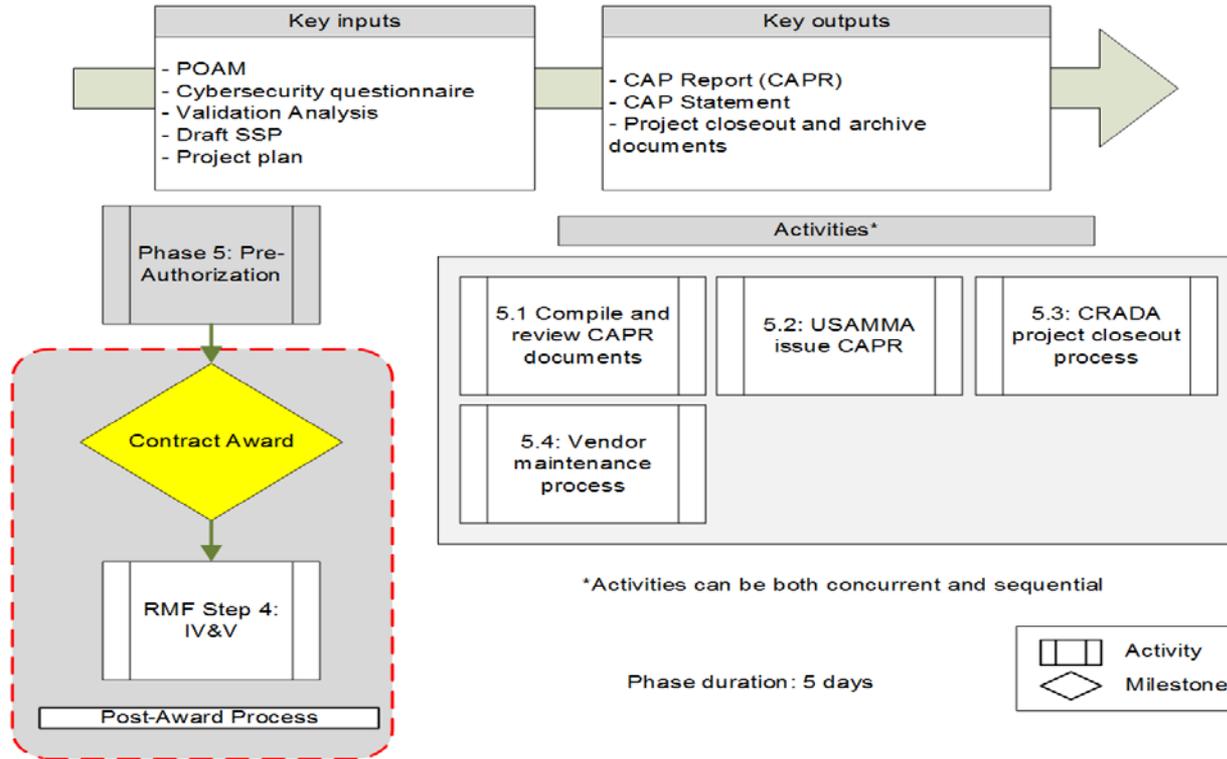
“Medically Ready Force...Ready Medical Force”

Phase 4: Validation



“Medically Ready Force...Ready Medical Force”

Phase 5: Pre-Authorization Determination & Maintenance



“Medically Ready Force...Ready Medical Force”

Summary

- DoD cybersecurity policies and programs create challenges to the existing medical device acquisition process
- USAMMA and DeltaStrac are developing a pilot process whereby vendors can get official Army sponsorship for cybersecurity assessment of their medical devices outside of a formal procurement process
- The Cybersecurity Assessment and Pre-Authorization (CAP) Cooperative Research and Development Agreement (CRADA) is designed to investigate the viability of this process
- CAP CRADA officially approved on 12 Jan 2016
- 1st Vendor enrolled April 2016

Key Takeaways

- Cybersecurity accreditation is currently a post-procurement/acquisition process
- The CAP CRADA is an investigative process
 - Formal RMF sponsorship prior to acquisition
 - Potentially shorten post-acquisition accreditation timeline
- CAP CRADA participation does not guarantee ATO

Questions?



Defense Health Agency

2016 Defense Health Information Technology Symposium

“Medically Ready Force...Ready Medical Force”

Evaluations



Defense Health Agency

2016 Defense Health Information Technology Symposium

Please complete your evaluations

“Medically Ready Force...Ready Medical Force”

Contact Information



2016 Defense Health Information Technology Symposium

MAJ Jonathan Deeter
Chief, Medical Device Cybersecurity
ICS-PMO, USAMMA
jonathan.p.deeter.mil@mail.mil

Gilroy Gotiangco
President, DeltaStrac, LLC
gilroy.gotiangco@deltastrac.com