UPGRADE

Universal **P**atchin**g** and **R**emediation for **A**utonomous **De**fense

Andrew Carney, Program Manager
Resilient Systems Office
Advanced Research Project Agency for Health

Have a question? Submit it to:

solutions.arpa-h.gov/Ask-A-Question/

ARPA-H

Cleared for Release

This ARPA-H document has been reviewed by the ARPA-H designated authority and has been cleared for public release.

UPGRADE Proposer's Day Agenda – June 20 (all times ET)

Time	Topic	Speaker
12:00 – 12:15	ARPA-H and RSO Overview	Andrew Carney
12:15 – 1:00	UPGRADE Program Overview	Andrew Carney
1:00 – 1:15	Guest Speaker - ASPR	Brian Mazanec
1:15 – 1:40	Solicitation Requirements	Marisa Meloney
1:40 – 2:00	Q&A (https://solutions.arpa-h.gov/Ask-A-Question/)	Andrew Carney
2:00	End	
2:10 – 6:00	Sidebars (5-minutes each, invite only)	Andrew Carney, Marisa Meloney

Cleared for Release

ARPA-H: The Mission

Advanced Research Projects Agency for Health (ARPA-H)

Andrew Carney, Program Manager
Resilient Systems Office

Cleared for Release

ARPA-H

Mission

Accelerate better health outcomes for everyone.

ARPA-H

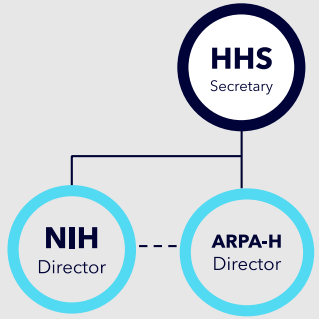
Cleared for Release

ARPA-H Key Features and Authorities

ARPA-H has unique structures and legal authorities that allow it to **function like a business – quickly, nimbly, and decisively**.

- ARPA-H is a **funding agency**
- **Independent** component of HHS within NIH; not an Institute
- No internal research labs; **disease agnostic**
- Generally **fund outcome-based contracts,** not grants; accelerated award timelines
- Unique **FDA reimbursement authority**
- **Appropriations,** budget independent from NIH

FY 2022	FY 2023	FY 2024	FY 2025
$1B	$1.5B	$1.5B	Request: $1.5B



Lean and nimble management structure with autonomy in decision-making.

ARPA-H Director **reports directly to HHS Secretary**

Term limits of 3-6 years bring urgency and idea flow.

Flexibility in hiring allows ARPA-H to recruit at levels competitive with industry.

Bottom-up decision-making. PMs have autonomy to make decisions quickly.

ARPA-H is a problems focused organization

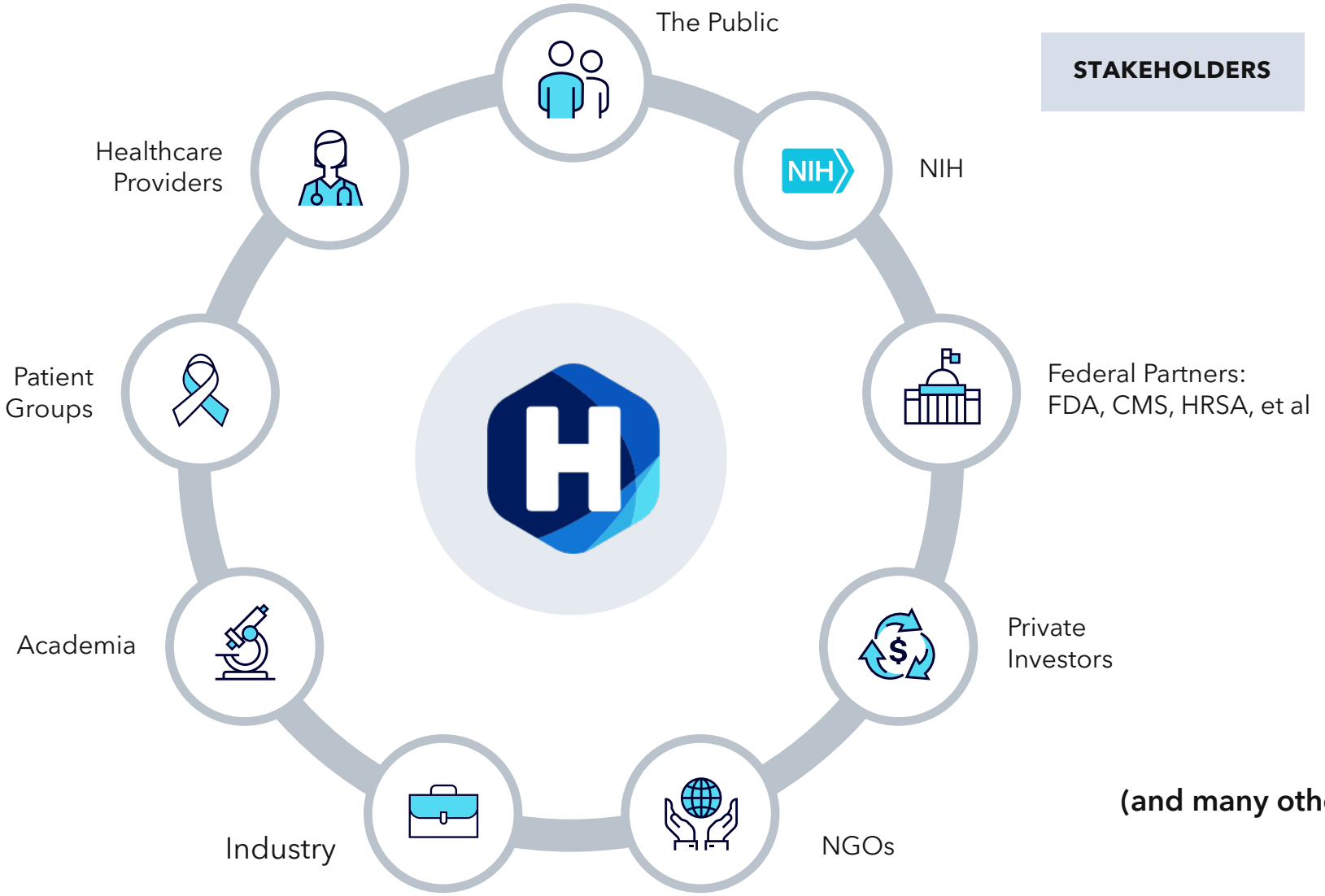
ARPA-H

Cleared for Release

ARPA-H Accelerates the Entire Health Ecosystem

CUSTOMERS

PERFORMERS



STAKEHOLDERS

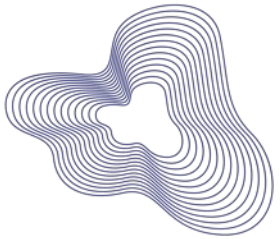
(and many others …)

ARPA-H

Cleared for Release

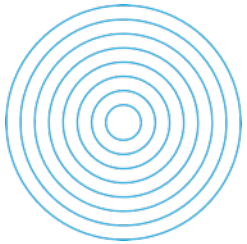
Initial Mission Focus Areas

Further ARPA-H investment in these areas will generate **asymmetrical benefits** to the health ecosystem



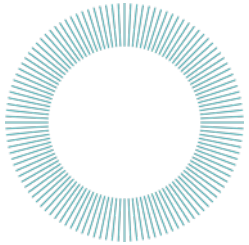
Health Science Futures

Expanding what's technically possible



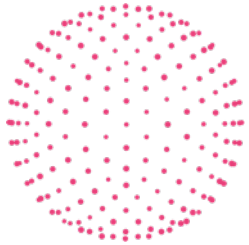
Scalable Solutions

Reaching everyone quickly



Proactive Health

Keeping people from being patients



Resilient Systems

Building integrated healthcare systems

Project Accelerator Transition Innovation

Ensuring programs survive in the wild

ARPA-H

Cleared for Release

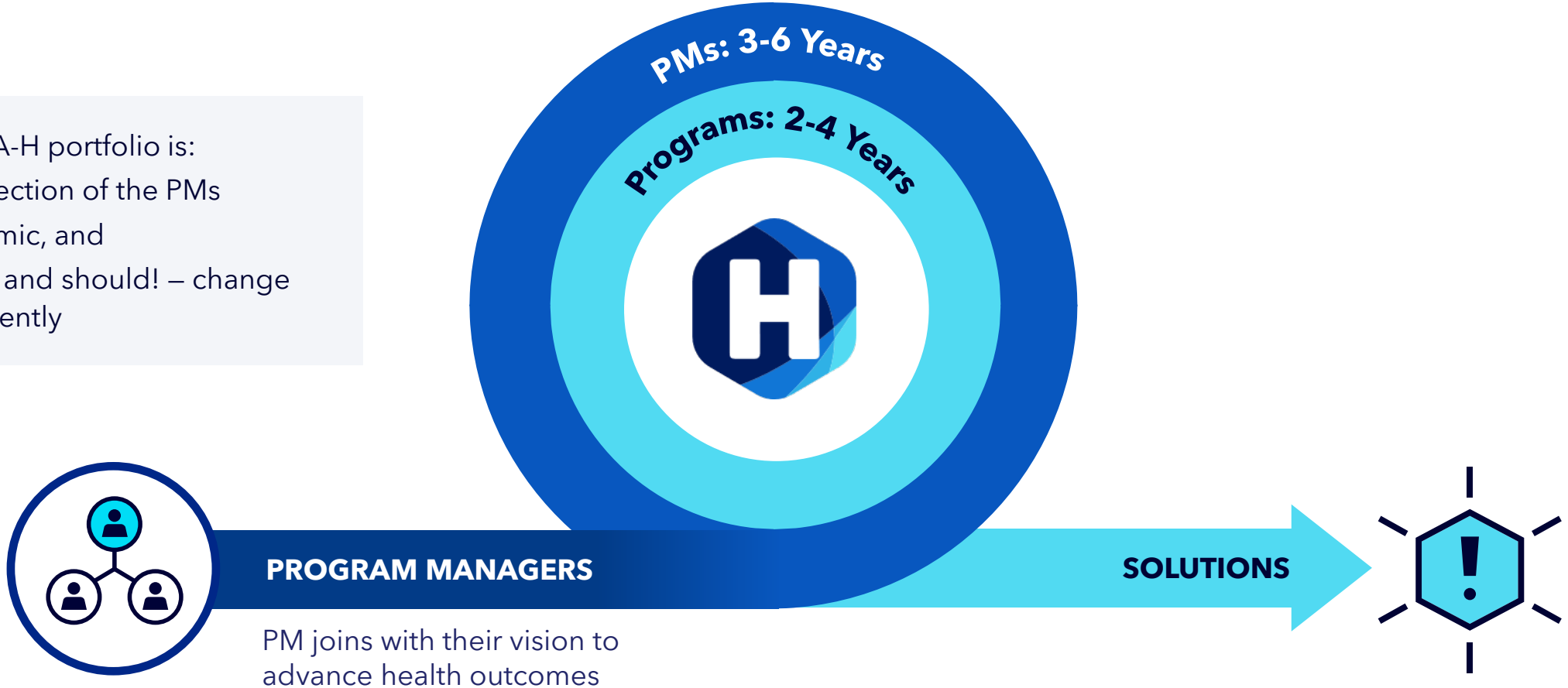
The Program and Program Manager Flywheel

The ARPA-H portfolio is:

(1) a reflection of the PMs

(2) dynamic, and

(3) will – and should! – change frequently



Cleared for Release

Program Lifecycle

From ideas to solutions in the real world

DESIGN PROGRAMS

- ARPA-Hard and well-defined problems in health
- Heilmeier Framework
- High risk/High consequence
- Stakeholder Insights

BUILD A PERFORMER TEAM

- Solicit Solutions from the community
- Find the best non-traditionals, industry, and academics to solve
- Build new coalitions

EXECUTE & MEASURE

- Active program management against metrics; PM = CEO
- Stakeholder engagement throughout to ensure transition
- Pivot resources when needed

LEARN & GROW

- Capture and share insights
- Technical honesty
- Advance the state of the art; 10x+ improvement, no incremental change

COMMERCIALIZE & TRANSITION

- Assist company formation or licencing
- Provide mentorship, connections to customers, investors
- De-risk investments

Cleared for Release

UPGRADE Overview

Universal **P**atchin**g** and **R**emediation for **A**utonon
Defense

Andrew Carney, Program Manager

Resilient Systems Office
Advanced Research Project Agency for Health

Cleared for Release

ARPA H

What if every hospital could autonomously protect itself and patients from cyber-threats?

ARPA-H

Cleared for Release

Cyber attacks threaten access to healthcare

HEALTH TECH

Rural Illinois hospital says 2021 ransomware attack partially to blame for closure

By **Dave Muoio** · Jun 13, 2023

Cyberattack forces Idaho hospital to send ambulances elsewhere

By Sean Lyngaas, CNN

Murfreesboro Medical Clinic closed due to 'sophisticated cyberattack'

Hospitals could be one cyberattack away from closure

Tina Reed, author of Axios Vitals

HEALTH TECH

UnitedHealth cyberattack impedes pharmacies' and hospitals' ability to process insurance claims

By Bob Herman, Brittany Trang, and Tara Bannow Feb. 23, 2024

ARPA-H

Cleared for Release

Trends & Impact

Cyber-attacks threaten hospitals and patient care

- **61%** of hospitals said ransomware affects their clinical care. **17%** said ransomware has led to **"serious patient harm."**
- **>370%** increase in the number of vulnerabilities that were weaponized last year
- **~50%** of hospital system downtime involved some form of cyber-attack in 2012-2018
- **$77.5B** in costs from healthcare cyber incidents since 2016, **$15B+** in 2023

Connected medical equipment and software are large vulnerabilities

- **96%** of hospitals use end-of-life operating systems, software, and medical equipment with known vulnerabilities
- **53%** of medical equipment currently contains critical vulnerabilities
- **Mission critical medical equipment** is often not remediated due to threat of downtime and **disruption in patient care**

Hospitals are not able to protect themselves or patients

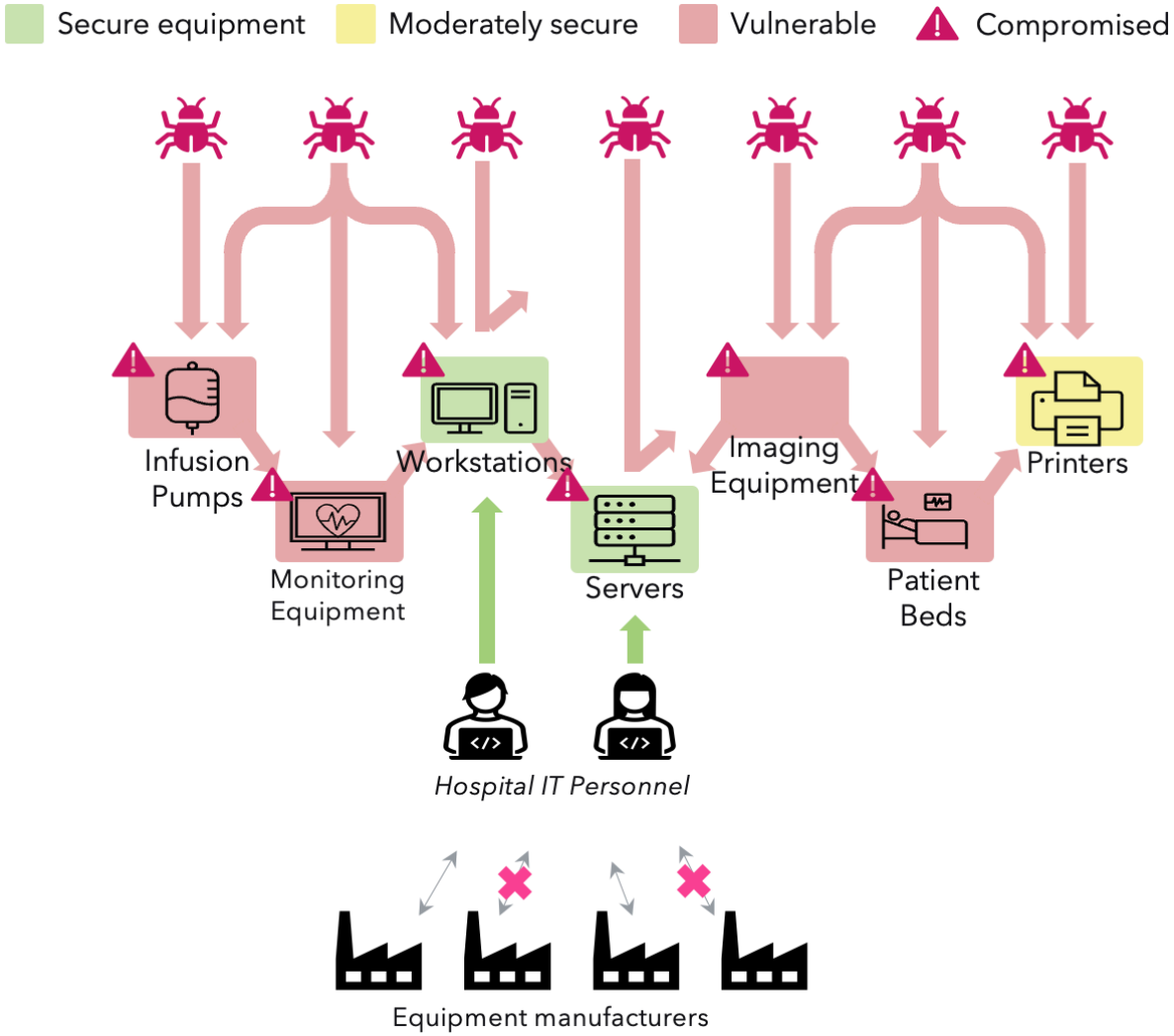
- **491 days** is the average time to apply critical security updates for hospital equipment (slowest compared to other sectors)
- **75%** of health IT failures resulting in patient death or harm are preventable.
- **28%** of healthcare cybersecurity jobs are unfilled and it takes **70%** longer to fill hospital IT positions

ARPA H

Cleared for Release

Today: Massive asymmetry between cyber attackers and hospital defense resources limits their ability to protect continuity of care

Vulnerabilities are common and many are not addressable



Today's limitations

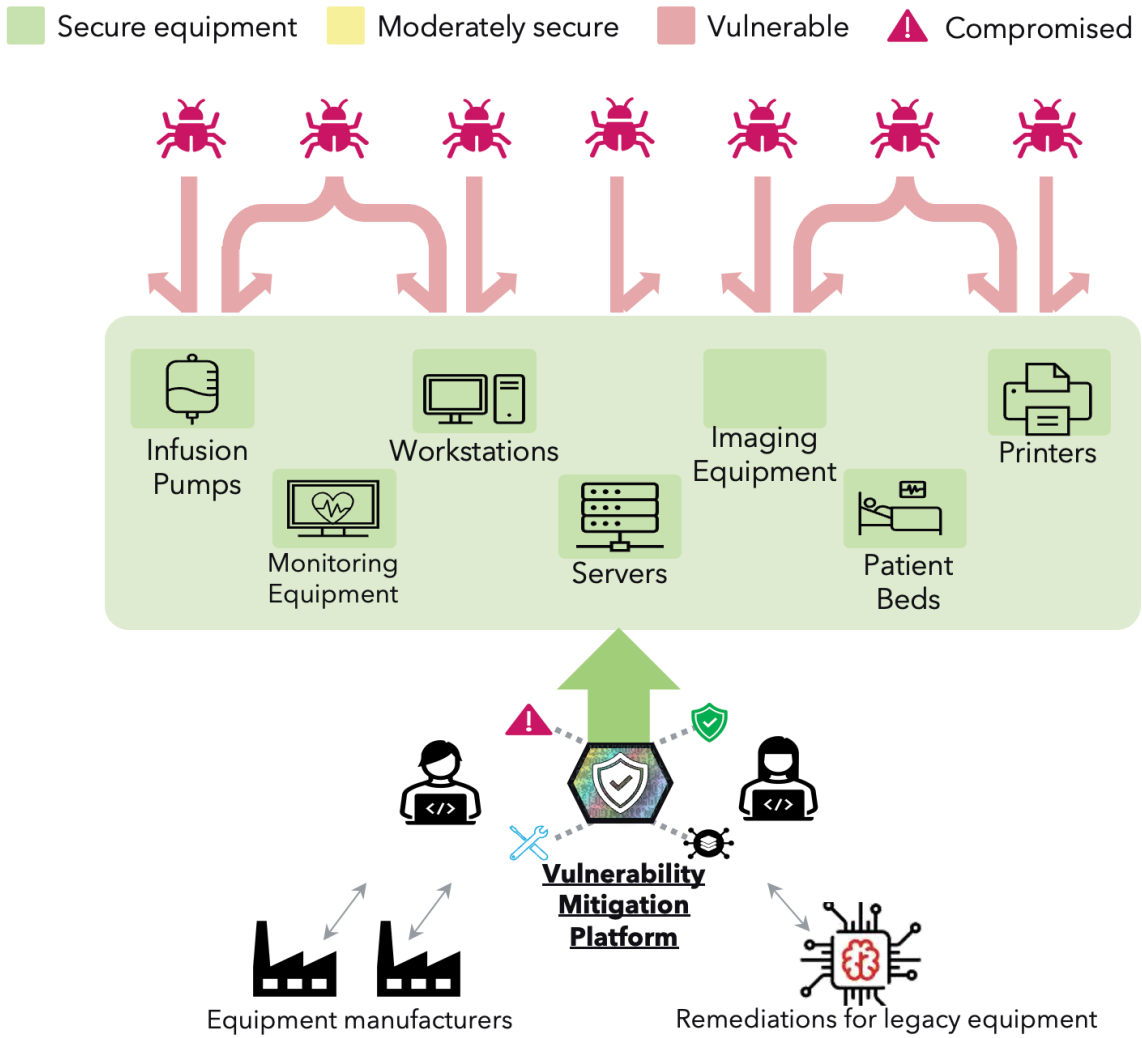
- Hospitals lack automated tools to find and fix vulnerabilities
- 20K+ pieces of connected hospital equipment per facility leads to incomplete tracking and remediation
- Detection of vulnerabilities is *ad hoc*, manual, and reactive instead of proactive
- Remediation development is slow and inconsistent
- Remediations for legacy equipment are unavailable
- No consistent mechanism to test remediations before deploying
- Deploying remediations to hospital equipment is slow and manual

ARPA

Cleared for Release

UPGRADE: Vulnerability Mitigation Platform enables hospitals to protect against cyberattacks and ensure continuity of care

Mitigation platform reduces attack surface and scales IT capability



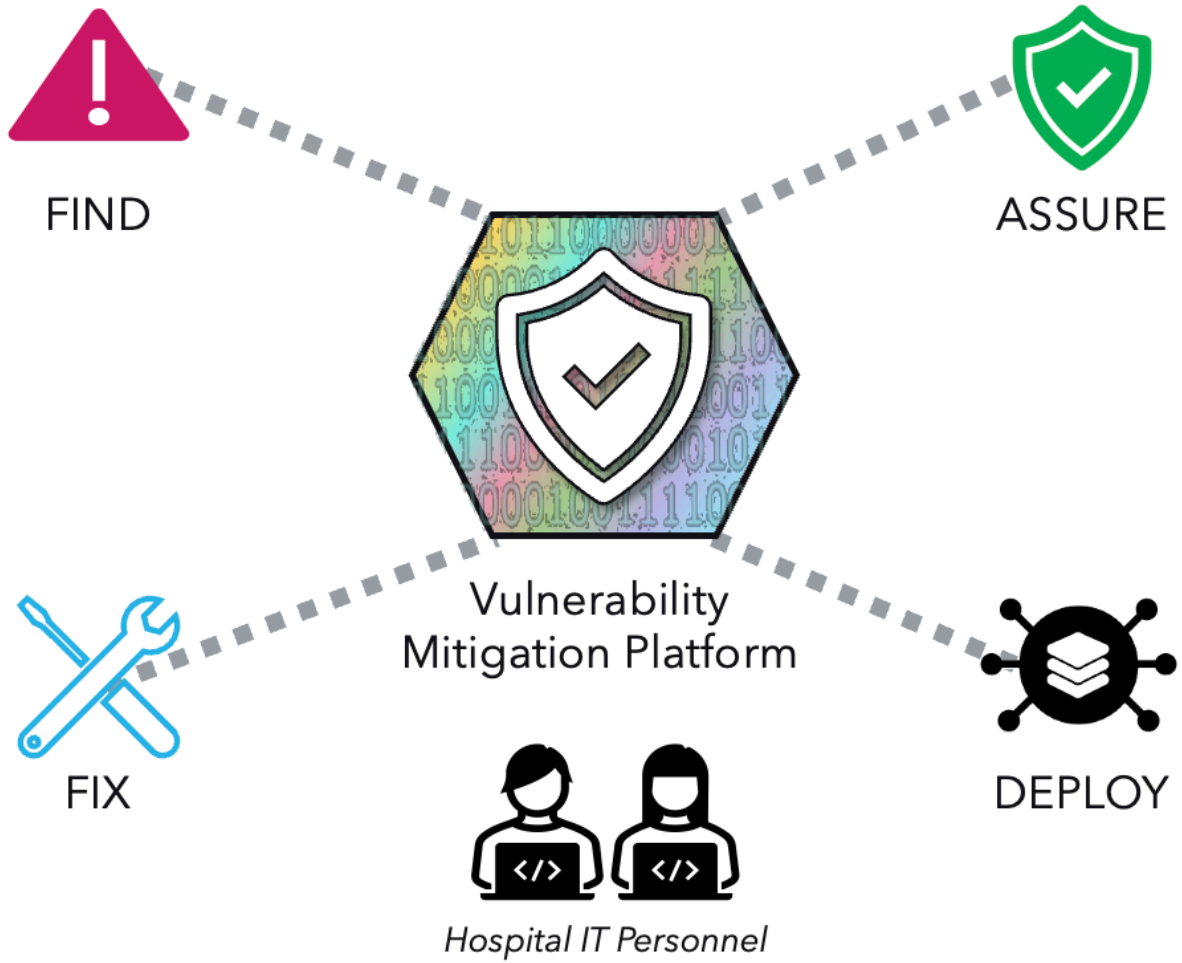
UPGRADE benefits

- Vulnerability Mitigation Platform enables hospitals to find and fix vulnerabilities faster
- Automated network mapping creates comprehensive understanding of equipment and environment
- Automated vulnerability detection proactively identifies security holes
- Equipment emulation accelerates vulnerability detection and remediation validation
- Accelerated remediation development generates high-assurance remediations
- Automated deployment of remediations to hospital equipment reduces uncertainty and manual effort

ARPA H

Cleared for Release

UPGRADE: Automated vulnerability remediation platform



Cleared for Release

UPGRADE: Automated vulnerability remediation platform

TA3: Automated Vulnerability Detection

FIND

ASSURE

TA2: Hospital Equipment Emulation

Vulnerability Mitigation Platform

TA4: Automated Remediation Development

FIX

DEPLOY

TA1: Vulnerability Mitigation Platform

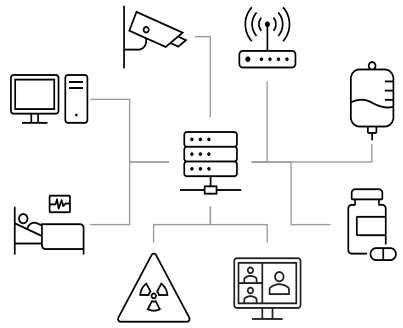
Hospital IT Personnel

ARPA H

Cleared for Release

UPGRADE: How it will work

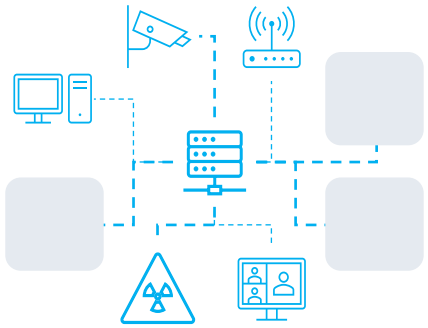
Vulnerable Real-world Hospital Network



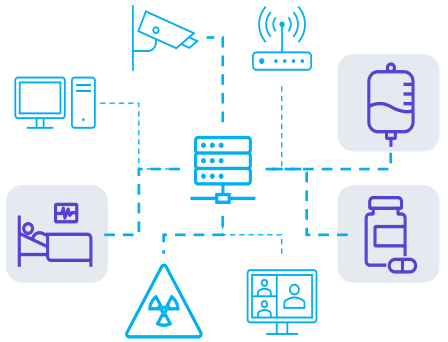
TA1: Map cyber-environment

Vulnerability Mitigation Platform (TA1)

TA1
Simulated Hospital Network
(*Missing some hospital equipment*)



TA2
Emulated Hospital Equipment
(*To include in the simulated network*)

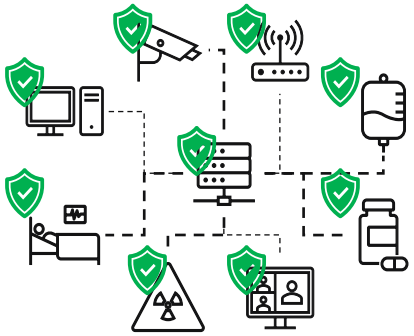


TA3
Proactive & Automated Vulnerability Detection

TA4
Proactive & Automated Remediation Development

TA1: Auto-Deploy remediations

Secure Real-world Hospital Network



UPGRADE will create a Vulnerability Mitigation Platform that enables hospitals to protect against cyberattacks and ensure continuity of care

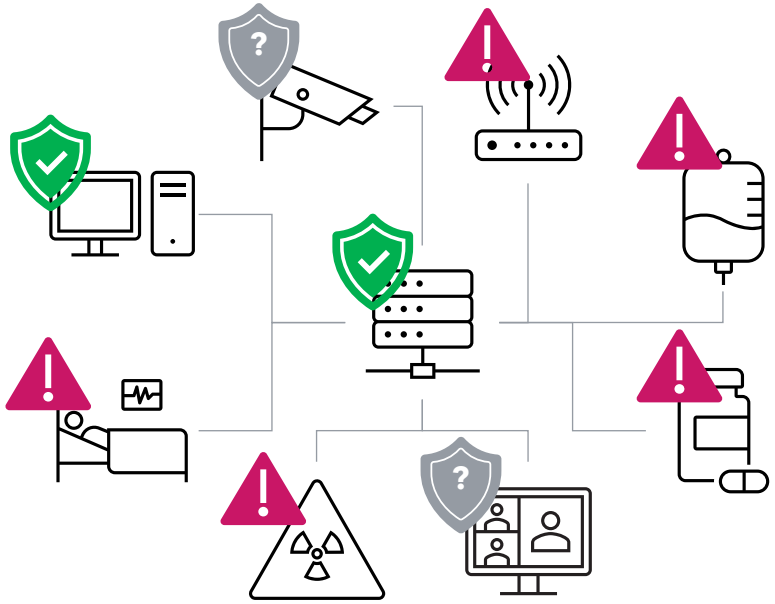
Challenges	UPGRADE Solution
Accurate system characterization	**TA1**: Cyber-environment Mapping & Simulation
Limited device understanding	**TA2**: Hospital Equipment Emulation
Reactive, time consuming, costly, expert-driven vulnerability detection	**TA3**: Automated Vulnerability Detection
Risky, slow, costly, and often impossible remediations	**TA4**: Automated Remediation Development
Hospital decision makers avoidance	**TA1**: Cyber Decision Support
Implementing remediations	**TA1**: Automated Remediation Deployment

Cleared for Release

TA1: Vulnerability Mitigation Platform

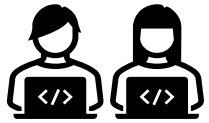
Goals: 1) Create a simulated hospital testing environment to mitigate impacts to real-world equipment. **2)** Develop cyber decision support tools to enable hospital decision makers to confidently initiate **3)** automatic remediation deployment tools.

BEFORE: Slow & Low-Confidence Remediation of Hospital Network *(if ever)*



> 490 days
for deployment of remediation

Vulnerability Mitigation Platform



Hospital IT Personnel

AFTER: High-Assurance Automated Deployment to Hospital Network

12 hours – 5 days
for deployment of remediation

Cleared for Release

TA1 Example Strong Performer

- Enables available remediation deployment/installation/configuration within hours of a vulnerability being discovered
- Clear, user friendly visibility into current state of patch deployment for medical devices and related technology within a hospital network
- An automated approach that scales to meet the current realities of hospital understaffing in information technology
- Provides stakeholders high confidence that mitigations will be effective, safe, and easily understood
- Assessment of existing tools and configurations as a baseline
- A confirmed hospital partner identified

Cleared for Release

TA1 Collaboration Table

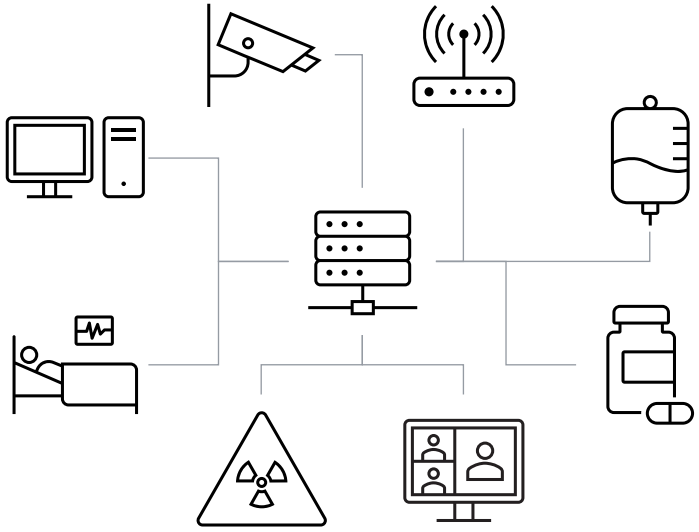
Partners	TA1 Performers will:
All	• In collaboration with ARPA-H, identify and align on specific hospital equipment (i.e. makes and models) that will be the targets of innovation throughout the program • Align on technical standards for all TAs (e.g., common data standards, formats, and specifications) to enable consistency and accessibility across all performers • Lay the foundation to enable platform extensibility after the end of the program
TA1	• Coordinate programmatic events with ARPA-H personnel and other TA1 performers to avoid scheduling and resource conflicts
TA2	• Integrate the emulated hospital equipment from TA2 into their WHS and VMP • Provide TA2 performers with access to the outputs from the cyber-environment mapping tool, their VMP, and their WHS for testing purposes
TA3	• Collaborate to include the TA3 vulnerability detection tools into their WHS and VMP • Ensure the severity & description of the vulnerabilities are accurately reflected in the Explainable Cyber Decision Support Tool • Provide TA3 performers with access to the outputs from the cyber-environment mapping tool, VMP, and WHS for testing purposes.
TA4	• Integrate the TA4 remediation tools into their WHS and VMP • Ensure the TA4 remediations are accurately described in the Explainable Cyber Decision Support Tool • Ensure that developed TA4 remediations are viable for deployment in an operational hospital environment • Provide TA4 performers with access to the outputs from the cyber-environment mapping tool, VMP, and WHS for testing purposes

Cleared for Release

TA2: Hospital Equipment Emulation

Goal: Emulate hospital equipment to speed vulnerability detection and creation of high-assurance remediations

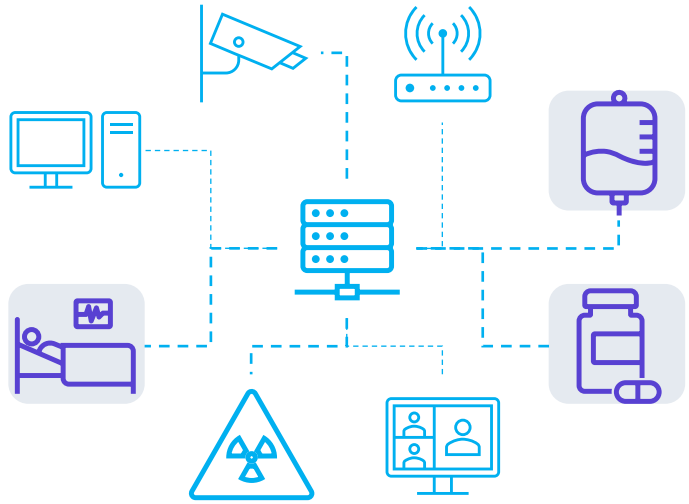
BEFORE: Real-world Hospital Network



Vulnerability Mitigation Platform

Hospital IT Personnel

AFTER: Simulated Hospital Network
(Includes hospital equipment)



The vulnerabilities & remediations for hospital equipment are **not well understood** because equipment is expensive to acquire / test.

Create **comprehensive** and **high-fidelity** digital twins of hospital equipment

Cleared for Release

TA2 Example Strong Performer

- Prioritizes emulation of core device functionality and external-facing services
- Has approaches that can be adjusted for degree of fidelity, runtime performance, cost to develop, etc.
- Accelerates the rate at which newly encountered medical devices are emulated
- Enables inter-device and inter-application interactions
- Provides high confidence to stakeholders that remediations will not negatively impact device operation or patient care

Cleared for Release

TA2 Collaboration Table

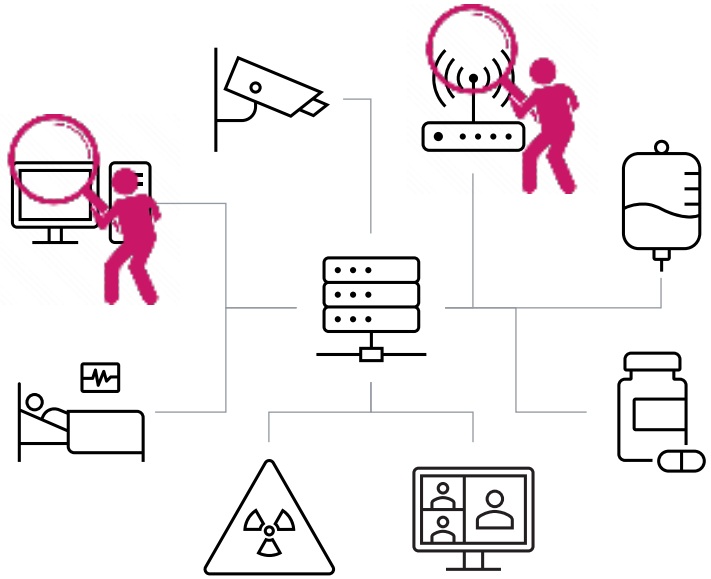
Partners	TA2 Performers will:
All	• In collaboration with ARPA-H, will identify and align on specific hospital equipment (i.e. makes and models) that will be the targets of innovation throughout the program • Align on technical standards for all TAs (e.g., common data standards, formats, and specifications) to enable consistency and accessibility across all performers • Lay the foundation to enable platform extensibility after the end of the program
TA1	• Integrate the emulated hospital equipment into the WHSs and the VMPs • Receive access to the outputs from the TA1 cyber-environment mapping tools, and access to the VMPs and WHSs for testing connectivity and behavior of the emulators within the WHS
TA3	• Share the complete emulators of the hospital equipment to enable TA3 performers to develop technologies to detect vulnerabilities • Allow TA3s to review of the initial hospital equipment emulation and solicit feedback necessary for TA3 to complete their deliverables
TA4	• Share the complete emulators of the hospital equipment that will allow TA4 performers to develop technologies to remediate vulnerabilities

Cleared for Release

TA3: Automated Vulnerability Detection

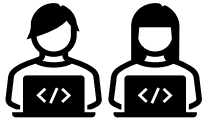
Goal: Proactively and automatically detect vulnerabilities in hospital equipment to enable remediation before a cyber-attack occurs

BEFORE: Reactive & Manual Vulnerability Detection



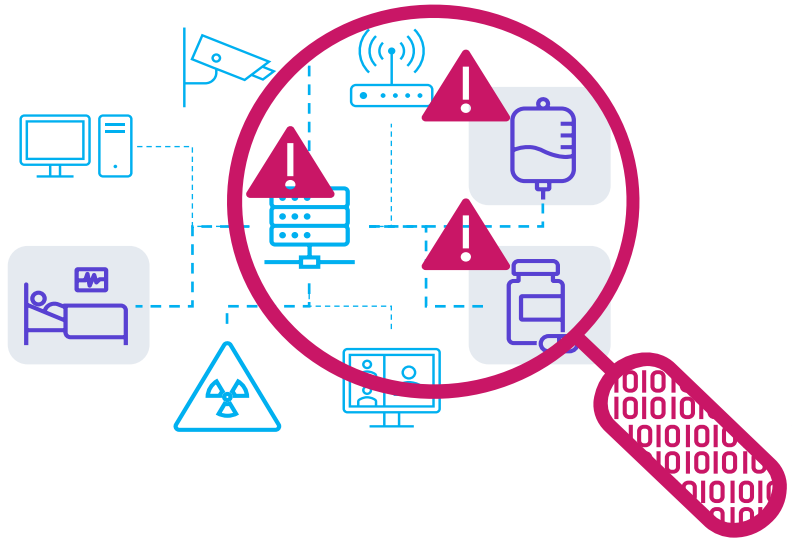
Reactive and **manual** discovery of vulnerabilities in **limited** equipment or networks

Vulnerability Mitigation Platform



Hospital IT Personnel

AFTER: Proactive & Automated Vulnerability Detection



Proactive and **automated** discovery of **novel** and known vulnerabilities in **all connected infrastructure**

Cleared for Release

TA3 Example Strong Performer

- Reasons over a wide array of medical devices and related technologies
- Uses novel discovery techniques informed by how human experts find vulnerabilities
- Prioritizes automated vulnerability discovery with targeted manual effort / human-in-the-loop workflows
- Has platform / architecture agnostic approaches
- Produces no false positives
- Considers impact of the network environment and other connected devices
- Is NOT limited to detecting known vulnerabilities

TA3 Collaboration Table

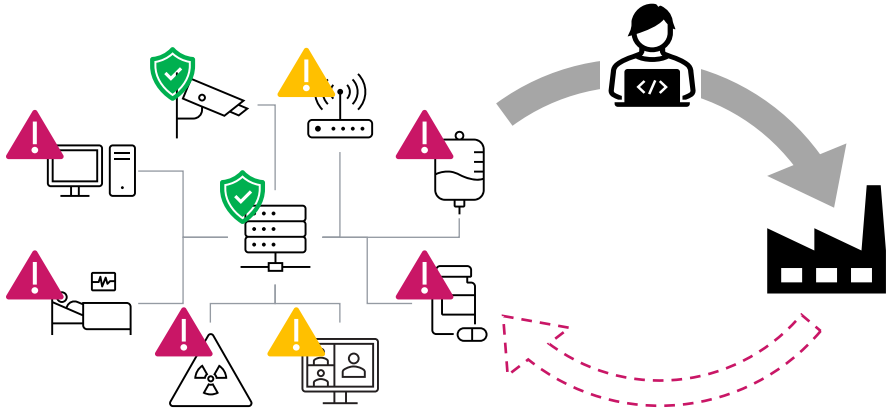
Partners	TA3 Performers will:
All	• In collaboration with ARPA-H, will identify and align on specific hospital equipment (i.e. makes and models) that will be the targets of innovation throughout the program • Align on technical standards for all TAs (e.g., common data standards, formats, and specifications) to enable consistency and accessibility across all performers the foundation to enable platform extensibility after the end of the program.
TA1	• Include the TA3 vulnerability detection tools into the WHSs and on the VMPs • Ensure the severity and description of the vulnerabilities are accurately reflected in the TA1 Explainable Cyber Decision Support Tool • Receive from TA1 performers access to outputs from the cyber-environment mapping tool, access to the VMPs, and access to the WHSs for testing purposes
TA2	• Review initial hospital equipment emulators and provide feedback necessary for the completion of TA3 deliverables • Ensure vulnerability detection tools function appropriately on TA2 emulators.
TA4	• Ensure that information about auto detected vulnerabilities (TA3) is effectively passed along to be used in the development of remediations for those vulnerabilities (TA4)

Cleared for Release

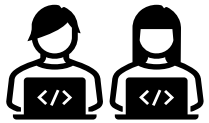
TA4: Automated Remediation Development

Goal: Automatic remediation development for detected vulnerabilities to enable rapid deployment (by TA1)

BEFORE: Reactive Manual Remediation Development



Vulnerability Mitigation Platform



Hospital IT Personnel

AFTER: Proactive & Automated Development of Remediations

Manual development of **highly generalized** remediations **90 days** after vulnerability is detected

Automated development of remediations within **hours** of detection that are **customized** for each use case

Cleared for Release

TA4 Example Strong Performer

- Does NOT interfere with patient care or negatively impact patient outcomes
- Automates remediation development to enable deployment within hours of a vulnerability being discovered
- Prioritizes automated vulnerability discovery with targeted manual effort / human-in-the-loop workflows
- Has platform / architecture agnostic approaches
- Supports legacy / end of life devices with minimal or no vendor resources
- Leverages natural language artifacts (e.g., documentation, GUI text)
- Prioritizes minimally invasive remediations
- Provides multiple remediation options for each discovered vulnerability

Cleared for Relase

TA4 Collaboration Table

Partners	TA4 Performers will:
All	• In collaboration with ARPA-H, will identify and align on specific hospital equipment (i.e. makes and models) that will be the targets of innovation throughout the program • Align on technical standards for all TAs (e.g., common data standards, formats, and specifications) to enable consistency and accessibility across all performers • Lay the foundation to enable platform extensibility after the end of the program.
TA1	• Include the remediation tools into the WHSs and on the VMPs • Ensure the remediations are accurately described in the TA1 Explainable Cyber Decision Support Tool and ensure that developed remediations are viable for deployment in an operational hospital environment • Receive from TA1 performers access to the outputs from the cyber-environment mapping tool, and access to their VMP and WHS for testing purposes.
TA2	• Receive complete emulators from TA2 performers, enabling TA4 performers to develop technologies to remediate vulnerabilities
TA3	• Share remediation outputs with TA3 to refine work product and technologies

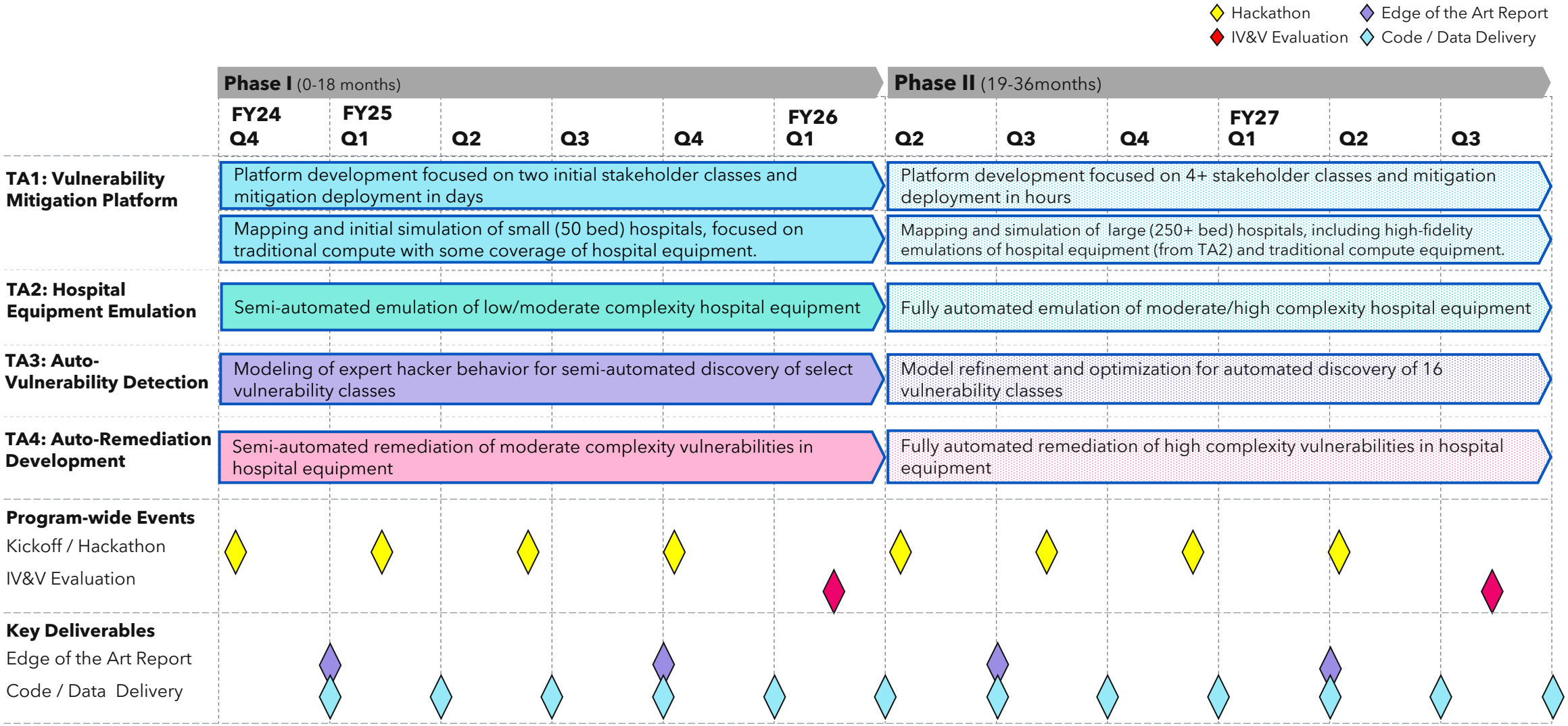
Cleared for Release

Key metrics for success

	Metric	Description	Phase I (0-18 mo)	Phase II (19-36 mo)
TA1: Vulnerability Mitigation Platform	**Remediation deployment time**	Mean time to deploy remediation (Current baseline is 471 days)	5 days	12 hours
	Target hospital environment	Can scale to hospital sizes that cover most of the U.S.	50 beds 2K+ devices (100% of critical access hospitals in US)	250 beds 10K+ devices (85% of total hospitals in US)
	Hospital environment fidelity	Environment's ability to represent the equipment, applications, and workflow of the target hospital	65%	95%
	Explainability	Enable multiple hospital stakeholders to make high confidence decisions based on explainable modeling of the hospital environment.	2 stakeholder roles (e.g., IT staff, hospital administration)	4 stakeholder roles (e.g., CISO, clinical staff)
TA2: Hospital Equipment Emulation	**Equipment emulator fidelity**	Emulator's ability to represent safety, security, and performance relevant processes and features	70%	90%
	Equipment emulator development time	Automating emulator development, normalized for number of hardware/software components	2x faster than control	20x faster than control
	Equipment classes	Encompasses common connected equipment found in hospitals	• Infusion Pumps • Patient Monitors • IP Telephones	• Imaging • Medication Dispensers
	Equipment class coverage	Coverage per class in target healthcare environments	40%	90%
TA3: Automated Vulnerability Detection	**Vulnerability discovery time**	Mean time to discover new vulnerabilities relative to a control human expert.	2x faster than control	100x faster than control
	Model accuracy / predictiveness	Expert process model accuracy (how predictive is the model for what is interesting to experts)	60%	99%
	Classes of vulnerability covered	# of classes (based on top 25 CWE lists)	4	16
TA4: Automated Remediation Development	**Remediation development time**	Mean time to develop new remediations relative to a control human expert.	3x faster than control	30x faster than control
	Remediation complexity	Successful remediation for a vulnerability with the following properties:	• Stateless • Static variables • Single device	• Stateful • Dynamic variables • Multi-device
	Performance impact	Ancillary impacts / graceful service degradation (Core functionality of the equipment must be unaffected)	< 40%	< 2%

Cleared for Release

Program Timeline & Milestones



ARPA H

Cleared for Release

Universal Patching and Remediation for Autonomous Defense (UPGRADE)

Vision: Develop an autonomous cyber-threat solution that enables proactive, scalable, and synchronized security updates, reducing the uncertainty and manual effort necessary to secure hospitals.

Technology focus areas:

1. Creation of a vulnerability mitigation platform
2. Creation of high-fidelity digital twins of hospital equipment
3. Auto-detection of vulnerabilities
4. Auto-developing custom defenses

Program Manager: Andrew Carney, Resilient Systems Mission Office

Key Dates

- Proposer's Day: June 20, 2024 | Virtual
- Solution Summary Due Date: July 11, 2024
- Proposal Due Date: September 18, 2024

ARPA H

Cleared for Release

What if every hospital could autonomously protect itself and patients from cyber threats?

ASPR Overview

Brian Mazanec, ASPR

Cleared for Release

ARPA-H

Acquisition Details

UPGRADE

Marisa Meloney
Agreement Officer
Business Innovation Division

ARPA H

Cleared for Release

PROPOSERS' DAY DISCLAIMER

- Only the information/instructions contained within the final Module Announcement counts!
- Proposals will only be evaluated in accordance with the instructions provided within the Master Announcement Instruction (MAI).

✓Read and review the draft UPGRADE module announcement
✓Check the Q&A frequently
✓Monitor SAM.gov and the UPGRADE program webpage for updates

Cleared for Release

ARPA-H Master Announcement Instruction (MAI) Basics

Master Announcement Instructions (MAI) and APRA-H UPGRADE Module Announcement

MAI is your manual and provides detailed instructions

MAI covers high-level instructions that are applicable to each Module Announcement

A Module Announcement provide project/program specific technical details.

Module Announcement has unique instructions specific to the Module.

The Module Announcement will refer to the MAI; have both documents available while writing proposal responses.

ARPA-H

Cleared for Release

UPGRADE Module Announcement Basics

Award Types

- Resulting awards will only be Other Transaction Agreements.
- Federal Acquisition Regulation (FAR) procurement contracts, Grants, and Cooperative Agreements should not be proposed.

Awards

- Multiple Awards are anticipated across the TAs.
- All conforming proposals will be evaluated in accordance with the evaluation criteria laid out in the MAI.

UPGRADE Timeline

- Draft Module Announcement posted: May 24, 2024
- Final Module Announcement posted: ~ End of June 2024
- Request for Solution Summaries Due Date: ~ June 11, 2024
- Proposal Due Date: ~ September 18, 2024

Technical Areas (TAs) & Program Timeline

TAs:

- TA 1: Vulnerability Mitigation Platform (VMP)
- TA 2: Hospital Equipment Emulation
- TA 3: Automated Vulnerability Detection
- TA 4: Automated Remediation Development

Program Phases:

- Phase I (Base period): 18 months
- Phase II (Option 1): 18

ARPA-H

Cleared for Release

UPGRADE Module Announcement Basics (cont.)

Module Categories

- BIT Module is ≤ $2,000,000
- BYTE Module is ≤ $4,499,999
- KILO Module is ≤ $10,000,000
- MEGA Module is ≤ $25,000,000
- GIG Module is ≤ $50,000,000

•Write to the scale and complexity of the effort.
  –Smaller efforts may be more exploratory or focused on a subset of the overall technical areas
  –Larger efforts may have more thorough technical descriptions, more milestones and details describing metrics

Stage Submissions

- Stage 1
  - Technical & Management
  - Basis of Estimate
  - Task Description Document
  - Administrative & National Policy Req.
- Stage 2
  - Price/Cost Proposal
  - Agreement Certification
  - Model Agreement

Bundle of Attachments

- One bundles of Attachments
  - Other Transactions

ARPA H

Cleared for Release

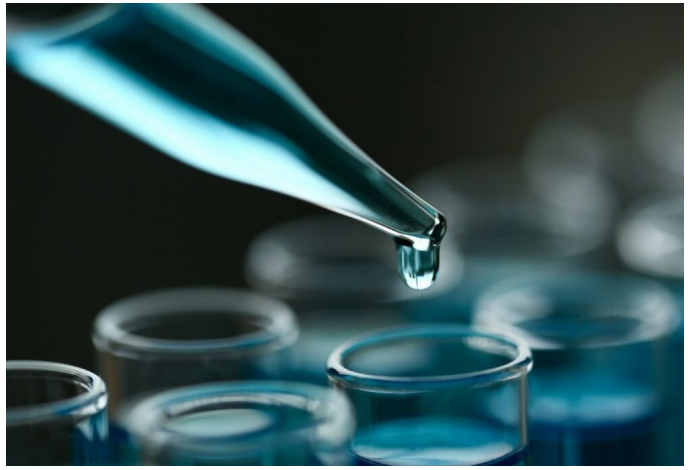
Award Types – Other Transactions (OTs)

What are OTs?

- ARPA-H has authority to award OTs when "*use of such authority is essential to promoting the success of the project*"
- OTs are Agreements (e.g., mutual assent, expressed by a valid offer and acceptance; adequate consideration; capacity; and legality)
- OTs reflect commercial contracting rather than traditional FAR procurement contracts

OTs are collaborative

- Increased collaboration and partnership, leading to more effective use of resources and knowledge sharing.
- Free-flowing negotiations and less restrictive than FAR based procurements.



Cleared for Release

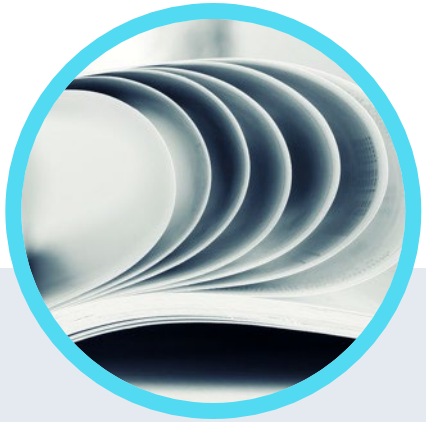
Other Transactions (OTs)

- **Pros:**
  - Many laws/regulations do not apply
    - Competition in Contracting Act; Bayh-Dole; 45 CFR 75; FAR/HHSAR; Cost Accounting Standards; Bid Protests, etc.
  - Invokes commercial practices, allowing for negotiating terms and conditions
    - May negotiate intellectual property (IP), payments, etc.
  - Streamlined award process

- **Cons:**
  - Lack the guardrails performers might desire under financial assistance or FAR contracts
    - Requires careful negotiation by sophisticated parties

Cleared for Release

Process Overview



Solution Summary Submission

- Are strongly encouraged – not required
- Content and submission instructions will be included within the final UPGRADE module Announcement (Appendix A)
- Should be submitted to https://solutions.arpa-h.gov ONLY
- Discourage/Encourage feedback

Proposals

- Government will encourage or discourage a proposal based on Solution Summary review. BUT – you can submit a proposal regardless of feedback received.
- Follow the stage submissions
- Content and submission instructions will be included in the final Module Announcement (reference Attachment 1 – OT bundles)
- Submit proposals to https://solutions.arpa-h.gov/Submit-Proposal/ ONLY

Evaluation and Selection

- The Government will review each conforming proposal against criterion 1-3 in descending order of importance.
- Stage 2 submissions will ONLY be requested if the technical volume has been selected.
- Selection for award will be made as outlined in the Master Announcement Instructions and ARPA-H UPGRADE Module Announcement.

ARPA-H

Cleared for Release

Evaluation Criteria

1

Overall Scientific and Technical Merit (Stage 1)

- Innovative, feasible, achievable, and complete
- An outcome that achieves the expected goals
- Technical risk(s) identification with a feasible mitigation strategy
- Intellectual Property (IP) rights structure; impact to Gov's ability to transition

2

Proposers' Capabilities and/or Related Experience (Stage 1)

- Team expertise and experience
- Experience in managing similar efforts

Cleared for Release

Evaluation Criteria (cont.)

3

Potential Contribution and Relevance to the ARPA-H Mission (Stage 1)

- Future application, including unmet needs within biomedicine and to improve health outcomes
- Potential for interdisciplinary approach

4

Price and Value Analysis/Cost Realism/Reasonableness (Stage 2)

- Price Reasonableness - Ensure the overall price is fair and reasonable (e.g., not too high no too low)
- Do prices reflect the technical goals and objectives of the solicitation and the proposed scope of work
- Value Analysis – what is the value of the research in comparison to the proposed price

Cleared for Release

Final Guidance

Monitor SAM.gov and Grants.gov

- Any/all changes to the MAI or Module Announcement will be made via formal amendments and posted online at SAM.gov
- No information discussed at Proposers' Day shall be construed as modifying the terms and conditions of the MAI or Module Announcement

Conform to all Requirements

- Thoroughly read the MAI and Module Announcement
- Non-conforming proposals **will not** be evaluated or considered for award
- Use the template documents provided. Use of these documents will speed up the Government's review of proposal submissions.

Important Information

- Visit for UPGRADE webpage for links to the draft and eventually the final module announcement, teaming page, Q&A.
- Use the Q&A process to communicate with the Government team.
- Submissions utilizing the solutions platform!
- UPGRADE Team webpage:
- Submissions and Q&A Portal:

ARPA-H

Cleared for Release

Q&A

Cleared for Release

ARPA H

Q&A

Q: Will the Proposers' Day slides/talks be posted online for those unable to attend?

A: Yes, the slides and a record of this Proposers' Day (PD) presentation will be posted to the UPGRADE website.

Q&A

Q: Is a Solution Summary required before submitting a full proposal?

A: No, proposer's are not required to submit a Solution Summary in advance of a proposal. However, proposer's are strongly encouraged to submit a Solution Summary in advance of a proposal as it’s a mechanism for potential proposers to obtain feedback prior to investing resources for a full proposal. ARPA-H will review Solution Summaries and respond in writing encouraging or discouraging the submission of a full proposal. Proposer's are able to submit a proposal regardless of the feedback received.

Q&A

Q: Who is allowed to submit a Solution Summary or full proposal?

A: As stated in the MAI, Section 2.1 "All responsible sources capable of satisfying the Government's needs may submit a proposal to a Module Announcement. Specifically, universities, non-profit organizations, small businesses and other than small businesses are eligible and encouraged to propose to Module Announcements." See additional details in Section 2.1.1 regarding FFRDC and Government Entity participation. The UPGRADE program anticipates teaming will be necessary to accomplish the UPGRADE goals and metrics.

Q&A

Q: What is the difference between a Solution Summary and a proposal?

A: Solution Summaries provide a synopsis of the proposed approach from a technical and budgetary perspective. The intent of the Solution Summary is to provide guidance on strategies that are within the scope of the program and that are likely to achieve program goals. Please note that the final UPGRADE module announcement will contain content and formatting guidance along with a template document to utilize (this will be Appendix A).

Proposals fully describe the technical approach, teaming, budget, etc. The final UPGRADE module announcement will contain template documents to be utilized in the proposal submission process (these will be provided within Attachment 1, Other Transaction Bundle).

Q&A

Q: Can an organization submit multiple proposals? Can an organization be part of multiple teams that submit multiple proposals?

A: Yes, organizations may be a part of multiple teams on multiple proposals. There are no limits, but proposers are requested to consider the most effective way for them to bring their expertise to the program.

Q&A

Q: How will proposals be evaluated?

A: Proposals will be evaluated in accordance with Section 4 of the Master Announcement Instruction, ARPA-H-MAI-24-01.

Q&A

Q: Who will own any intellectual property generated from the program?

A: The ARPA-H UPGRADE program will emphasize creating and leveraging open-source technology and architectures. Intellectual Property rights asserted by proposers are strongly encouraged to be aligned with open-source regimes. For Other Transaction Agreements, IP will be subject to negotiations between the proposer and ARPA-H. ARPA-H seeks to ensure IP restrictions do not impede the application of breakthrough technologies to the people who can benefit from these technologies. See Section 2.F. of the UPGRADE MAI for more information on Intellectual Property.

Q&A

Q: Is teaming required? Will the program manager/team assist in suggesting teaming?

A: While teaming is not required, it is strongly recommended that proposers seek out the strongest possible team member for each of the technical areas (TAs). This will ensure that all program goals are met.

We have created a teaming page (https://arpa-h.gov/research-and-funding/programs/upgrade/teaming) where prospective performers can share their profiles and learn about other interested parties. Note: The UPGRADE team will not suggest or direct teaming.

Q&A

Q: In the draft solicitation, section C. PROGRAM STRUCTURE AND INTEGRATION states: Proposers may submit a single proposal which addresses any TA singly or any combination of TA1, TA2, TA3, and/or TA4; proposers should NOT submit multiple proposals if proposing to more than one TA. Does "proposers" refer to proposal teams (individuals) or organizations? Is an organization (e.g., a university) limited to one proposal submission total, or is the submission limit on individual teams (i.e., the same team cannot submit more than one proposal)?

A: Proposers refers to proposed teams, organized by the prime proposer. If the proposing team is interested in proposing to more than one TA, then there should be one proposal submision. Organizations can be on multiple teams, and the same team can submit more than one proposal if the technical solutions are separate and distinct.

Cleared for Release

Q&A

Q: Would an analysis of an ongoing attack (e.g. to detect a vulnerability already being exploited, or to discover vulnerability the attacker may be planning to exploit next after pivoting from an already-compromised system) be in scope for this technical area?

A: Discovery and remediation of vulnerabilities in devices and systems currently deployed in hospitals is in scope for this program. However, direct analysis of ongoing attacks is not considered in scope for this program.

Q&A

Q: Will UPGRADE (TA-1) be made available to non-hospitals, e.g., health insurance organizations such as carriers and platform providers?

A: UPGRADE's aim is to secure complex and unique hospital networks that contain a plethora medical devices, traditional IT and OT assets, etc. Hospitals are the focus but knowledge gathered through this research will likely be beneficial and applicable across other industries.

ARPA H