MODULE ANNOUNCEMENT

FOR

UNIVERSAL PATCHING AND REMEDIATION FOR AUTONOMOUS DEFENSE (UPGRADE)

ARPA-H-MAI-24-01-05

JULY 2, 2024

CONTENTS

UNIVERSAL PATCHING AND REMEDIATION FOR AUTONOMOUS DEFENSE (UPGRADE)

A. MODULE ANNOUNCEMENT OVERVIEW INFORMATION

FEDERAL AGENCY NAME: Advanced Research Projects Agency for Health (ARPA-H)

MODULE ANNOUNCEMENT TITLE: Universal PatchinG and Remediation for Autonomous DEfense (UPGRADE)

ANNOUNCEMENT TYPE: Initial Announcement

MODULE ANNOUNCEMENT NUMBER: ARPA-H-MAI-24-01-05

DATES: (All times listed herein are Eastern Time)

- *Draft Module Announcement release date*: 05/24/2024
- *Final Module Announcement release date*: 07/02/2024
- *Proposer's Day:* 06/20/2024
- *Solution Summaries due date:* 07/22/2024
- *Questions & Answers (Q&A) due date*: 08/16/2024
- *Questions and Answers (Q&A) release date:* 09/04/2024
- *Proposal due date*: 09/18/2024

B. OPPORTUNITY DESCRIPTION

1. The mission of the Advanced Research Projects Agency for-Health (ARPA-H) is to accelerate better health outcomes for everyone by advancing innovative research that addresses society's most challenging health problems. Awardees will develop groundbreaking new ways to tackle health-related challenges through high potential, high-impact research. ARPA-H seeks proposals to develop a revolutionary new cybersecurity platform to enable hospitals and health systems to protect themselves from cyberattacks. The Universal PatchinG and Remediation for Autonomous DEfense (UPGRADE) program will empower hospital information Technology (IT) teams to protect health systems from cyberattacks and ensure continuity of patient care without requiring additional personnel or manual effort. Modern U.S. hospitals are characterized by massive complexity and low IT resourcing, indicating the need for revolutionary ways to scale the breadth and quality of healthcare cyber-defenses, especially related to the thousands of unsecured internet-connected devices found in every hospital.

2. UPGRADE aims to fund the creation of vulnerability mitigation tools that act as a force multiplier for hospital IT/cybersecurity teams, dramatically advancing hospitals' capacities to understand, source, plan, and deploy security upgrades for connected hospital equipment (e.g., equipment germane to hospital environments including but not limited to infusion pumps, patient monitoring equipment, and imaging equipment). UPGRADE envisions a semi-autonomous cyber-threat mitigation platform that enables proactive, scalable, and synchronized security updates, adaptable to any hospital environment, and across a wide array of the most vulnerable equipment classes. This software platform will contain a suite of tools that enable proactive evaluation of potential vulnerabilities, and how corresponding security updates might impact hospital operations. This will empower hospital decision makers to deploy security remediations without risking the real-world operational downtime that threatens the continuity of patient care. UPGRADE will unify these technologies, which span numerous cybersecurity and healthcare disciplines, into a user-friendly platform that is paired with an integrated cyber-decision support tool. This integrated platform will provide hospitals with critical decision-making insights, including tools to comprehensively map a hospital's cyber environment, automated explainability technologies to characterize cost-value trade-offs for cybersecurity experts and hospital administrators, and methods to auto-deploy security updates (i.e., "remediations") for equipment that historically lacks these mechanisms.

C. BACKGROUND CONTEXT

1. Cyberattacks are a significant and growing threat to U.S. medical facilities and patient care. Even short disruptions to IT systems can critically impair patient services and contribute to hospital closures. For example, in February 2021 St. Margaret's Health, a hospital in rural Illinois, experienced a ransomware attack that shut down its IT systems including email, electronic medical records, and billing for four months. This had an immediate and prolonged impact on patient care. Ultimately, the delays in billing, combined with the fact that many insurance plans have timely filing clauses and thus do not pay late claims, forced the hospital to close in June of 2023.[1]

2. The 2024 cyberattack at Change Healthcare, the world's largest facilitator of health and medical data, is another unfortunate example of the widespread devastation a cyberattack can cause. Hundreds of thousands of physicians, dentists, and thousands of hospitals and pharmacies lost access to health insurance information for 24 days causing delays in continuity of care and disrupting access to life-saving medications. Many patients were forced to pay full price for their life saving medications with no assurance of whether they would

eventually be reimbursed and on what timeline. In addition, it is estimated that some health care providers lost more than $100 million in revenue per day because of the outage. [2] UnitedHealth Group is currently working through a $14 billion backlog in medical claims. [3]

3. Hospital cyberattacks are typically carried out through vulnerabilities in IT systems, which encompass all internet-connected equipment. In many industries, IT systems are predominantly comprised of "traditional compute" devices (e.g., laptops, servers, routers, etc.), whereas hospital IT systems are heavily comprised of "non-traditional" connected hospital equipment, which are critical for patient health and safety and include infusion pumps, patient monitoring equipment, imaging equipment, laboratory information systems, and other software-enabled devices unique to the healthcare sector. Hospital equipment vulnerabilities are pervasive; 53% of all hospital equipment currently contain critical vulnerabilities and 96% of hospitals contain equipment with these vulnerabilities[4].

4. One of the key defenses against cyberattacks is regular equipment remediation – e.g., deploying security updates to prevent unwanted manipulation by external actors. The remediation of vulnerabilities in hospitals has proven exceedingly difficult, driven by several key factors: hospitals can contain tens of thousands of internet-connected devices, making coordinated management of the cyber-environment exceedingly difficult to execute; hospital equipment is created by a wide variety of different vendors who do not disclose hardware and software specifications, so hospital IT teams have little insight into device operations and modifications; and hospitals have low tolerance for any equipment down-time for remediation and testing.

5. Currently, IT teams are not equipped to protect hospital operations or continuity of patient care due to limited healthcare IT workforces and resources. 28% of healthcare cybersecurity jobs are unfilled and it takes 70% longer to fill hospital IT positions as compared to other industries[5]. No tools exist that would allow hospital IT teams to safely develop, test, and deploy the remediations necessary to secure hospital equipment. It currently takes hospitals 491 days on average to apply critical security updates for hospital equipment, even when the vulnerabilities are known[6]. This is by far the slowest compared to other sectors, which deploy critical security updates in a matter of days or weeks. Software updates are further complicated by the fact that hospital equipment includes "legacy equipment," where the manufacturer no longer supports software upgrades.

6. NATIONAL HEALTH IMPACT

(a) Hospitals are a vital component of our nation's critical infrastructure and uniquely vulnerable to cyber threat actors. For example, 61% of hospitals have stated that ransomware has affected their clinical care, with 17% saying ransomware has led to serious patient harm[7]. Between 2012 and 2018 roughly 50% of hospital system downtime involved some form of cyber-attack[8]. Since 2016, cyber incidents have cost the healthcare industry $77.5B, with over $15B in 2023 alone[9]. Beyond immense cost and disruption to health system operations, cyberattacks also threaten the security and privacy of patient medical records. Individual successful cyberattacks have stolen hundreds of thousands of medical records and over 95% of identity theft is traceable to stolen medical data[10]. Reducing the frequency and impact of cyberattacks against hospitals will prevent targeted disruptions to operational continuity, improve patient outcomes, and prevent loss of life. The effective capacity of hospitals will be increased through improved facility uptime. At present, hospital ransomware attacks are intensely disruptive, with these hospitals resorting to pulling their entire systems offline, switching to manual records, diverting patients to other hospitals, and halting billing for unpredictable periods, ranging from days to months. Concurrently, hospitals commonly incur substantial costs for forensics, remediation, and in some cases ransom costs. These cascading effects can cripple a hospital and even force it to close permanently[11].

(b) On average, U.S. hospital organizations invest 0.37% of their revenue in cybersecurity, which is *8x lower* than the average investment of all other industries and *23x lower* than the financial sector, which also handles and stores large volumes of sensitive data[12]. Manual IT operations are expensive, slow, and cannot compete with fully automated cyber attackers. Remediation deployment is difficult to schedule, and the impact of changes is hard to predict, resulting in a reluctance by hospitals and equipment manufacturers to issue remediations. Healthcare computer networks are complex and far more heterogenous than most other industries. Due to the heterogeneity of the hospital environment, the need to remediate systems without downtime, and the scarcity of specialized hospital equipment expertise, the health sector requires vulnerability mitigation tools that are effective, scalable, and fast to implement.

7. CHALLENGES UNIQUE TO THE HEALTHCARE SECTOR

(a) The health sector faces numerous compounding challenges preventing hospitals from leveraging the technological advances that have revolutionized the speed and comprehensiveness of cybersecurity protections that allow other industries to be more resilient to cyberattacks. For one, the health sector lacks the means to test healthcare IT in a representative environment. The virtualization tools used today to create digital twins (e.g., QEMU, VMware) predominantly support common consumer devices and do not support the thousands of different pieces of hospital equipment necessary to create an emulated test environment useful for hospitals[13]. Manual creation of these hospital equipment emulators is not a viable option as the process is labor intensive and hundreds of new pieces of hospital equipment enter the market each month. Exacerbating the issue, the scale and dynamism of health environments makes it difficult for most hospitals to maintain situational awareness of all the connected equipment within their cyber-environments. The connected equipment footprint can be massive, entailing over 20,000 pieces of hospital equipment alone in some large hospital systems[14].

(b) Vulnerability detection is a slow, imperfect, and expensive process. Today, it takes vulnerability researchers hundreds or thousands of combined hours of manual effort to identify a single flaw in a piece of equipment[15]. Each flaw may have been present in the equipment for 4+ years before discovery, creating a significant window of opportunity for an attacker to discover and exploit this and other flaws. The long window of vulnerability exacerbates the asymmetry of cybersecurity, where threat actors only need a handful of vulnerabilities to achieve their goals while successful defense requires knowledge of all vulnerabilities in a system. Once vulnerabilities are found, remediation is an inefficient, manual process. The current vulnerability "debt" in health care is considerable, with 993 vulnerabilities found in hospital equipment in 2023 alone, 160 of which have publicly available exploits[16]. The current development cycle for vendor-initiated remediation takes 30-90 days (or more) and focuses only on single pieces of equipment without consideration for impacts to adjacent systems[17]. Compounding matters, 73% of hospitals rely on legacy operating systems which no longer receive manufacturer support, thus increasing critical vulnerability as there is no clear path to remediation[18].

(c) Remediation deployment involves significant delays, due to risk aversion, resource limitations, and availability of security remediations. It currently takes 491 days on average to apply critical security updates for hospital equipment, which was the slowest compared to other industries from 2018-2022[19]. Reasons behind these delays are include: high-risk of significant system downtime because the impacts and side-effects of deploying a remediation are unknown; there is often low confidence and/or understanding among key hospital stakeholders (e.g., Chief Information Security Officer (CISO), Department Head, System Administrators) for why the remediation is necessary, and if it will resolve the vulnerability without causing other disruptions; there is a scarcity of qualified hospital IT personnel to deploy remediations for thousands of connected pieces of hospital equipment per facility, and limited support from equipment manufacturers to assist in the deployment process.

D. PROGRAM DESCRIPTION

1. UPGRADE aims to develop integrated Vulnerability Mitigation Platforms (VMPs) that enable critical access hospitals to eliminate cyber vulnerabilities and preserve continuity of patient care. The platforms will act as a force multiplier for hospital cybersecurity teams by expediting their ability to comprehensively characterize their hospital's cyber network, identify vulnerabilities within that network, source remediations to mitigate the vulnerabilities, and accelerate remediation deployment. At its core, the platforms will create a digital twin of a hospital's cyber environment to accelerate vulnerability detection, evaluate novel remediations, and help cybersecurity teams prioritize remediation deployment.

2. If successful, UPGRADE platforms will give hospital IT teams an unprecedented ability to validate remediations before they are deployed. To maintain continuity of patient care, hospitals need assurance that security upgrades are functionally correct and satisfy appropriate safety and security properties. To meet this need, UPGRADE will focus on high-assurance security updates as well as digital twin capabilities that enable hospital IT to understand how security upgrades will affect hospital operations. The digital twin capabilities at the heart of the UPGRADE platforms will provide dual benefits by accelerating vulnerability detection and assuring that remediations meet strict safety and security criteria.

3. Automation also plays a key role in accelerating cyber defense activities. Therefore, the UPGRADE platforms will include decision support capabilities that provide IT teams and relevant hospital administrators with the context they need to make informed decisions about emerging vulnerabilities, novel remediations, and secure network configurations. Because hospital IT teams must secure

hospital networks while also maximizing the uptime of hospital infrastructure, the platforms will include automated explanation techniques that provide context about the vulnerabilities, properties of the high-assurance remediations, and remediation validation results.

E. TECHNICAL AREAS (TAS)

1. INTRODUCTION. UPGRADE seeks to develop a suite of autonomous vulnerability mitigation tools that enable hospitals of varying sizes and complexity to protect continuity of patient care by implementing strong, proactive cybersecurity. These capabilities will be integrated into a VMP. Due to significant advances in the use of artificial intelligence and machine learning (AI/ML) in cybersecurity technologies, tremendous opportunities exist to develop automated systems that improve the security of legacy hospital equipment and hospital networks. These innovations will enable a proactive approach to identifying and mitigating potential vulnerabilities.

2. SUMMARY OF TECHNICAL AREAS. The UPGRADE Program consists of four interconnected TAs; a high-level review of each TA is outlined immediately below (and in Figure 1) and followed by a comprehensive description of each TA thereafter.

   (a) TA1: Vulnerability Mitigation Platform (VMP): TA1 performers will each develop, evaluate, and field test a VMP, which will host a suite of tools that enable hospital IT teams to more effectively secure hospital equipment at scale. Using the platforms, TA1 performers will demonstrate capabilities that deploy remediations while protecting hospital operations and continuity of patient care. In parallel, TA1 performers will establish representative Whole-Hospital-Simulation (WHS) environments that include both physical equipment and digital equipment emulators (from TA2) that mimic real-world, operational hospital networks. These WHSs will serve as sandboxes for rapid development and testing of innovations across all TAs in UPGRADE. TA1 performers will partner with and be the primary liaisons for at least one operational hospital to ensure the platform tools are designed around the needs of under-resourced hospital IT teams. As such, TA1 will serve as a system integrator for TA2-TA4 to ensure that the interfaces for the component technologies meet the needs of hospital IT teams as well as non-technical hospital administrators who have a vested interested in preventing cyber-attacks.

   (b) TA2: Hospital Equipment Emulation: TA2 performers will create digital twins/emulators of hospital equipment that can be leveraged by other

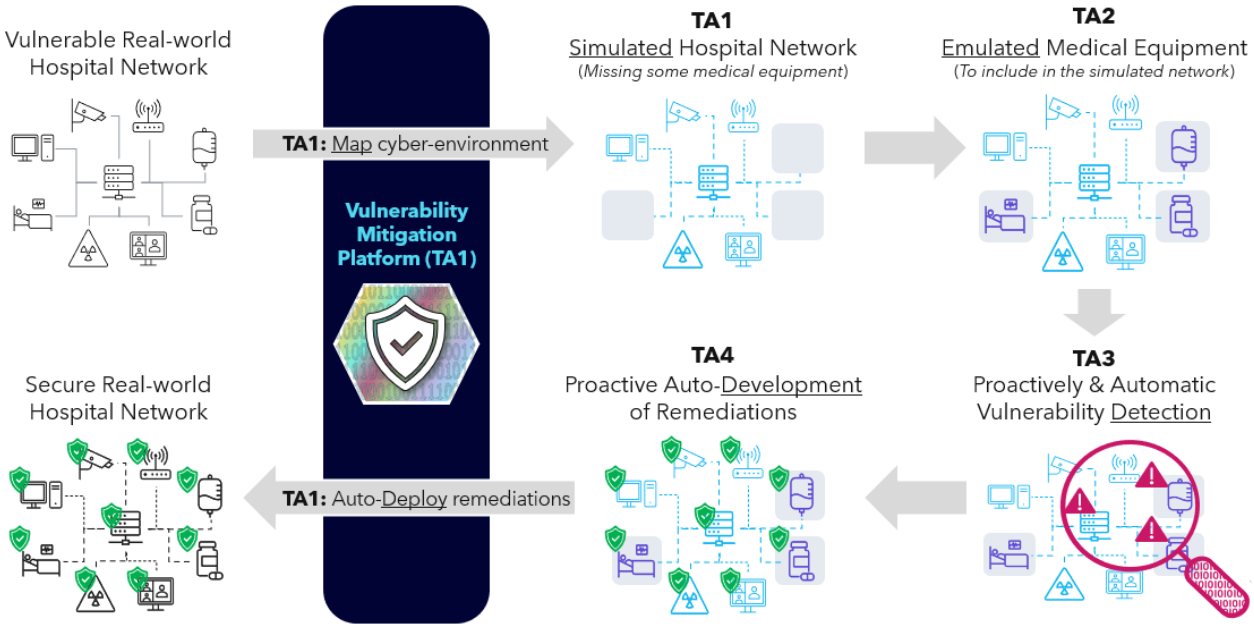
TAs for equipment-specific vulnerability detection, remediation development, and incorporation into WHSs (which also includes "traditional compute" and the unique configurations of hospital networks). TA2 hospital equipment emulators will play a crucial role in accelerating vulnerability detection from TA3 and validating high-assurance remediations from TA4.

(c) TA3: Automated Vulnerability Detection: TA3 performers will develop software tools that enable proactive and autonomous identification of vulnerabilities in hospital equipment, leveraging the WHS developed by TA1 performers, emulators from TA2, and if necessary, physical hospital equipment (purchased by the TA3 performer).

(d) TA4: Automated Remediation Development: TA4 performers will create autonomous capabilities to develop high-assurance remediations to vulnerabilities identified by TA3. The remediations will feed into the VMPs (TA1) so that they can be presented to hospital decision makers. Decision makers should receive both the remediations as well as information about the assurance evidence to facilitate decisions regarding the automated deployment of remediations within the operational (real-world) hospital.

3. UPGRADE PROGRAM OVERVIEW. Together, the TAs will support the following workflow, highlighted in
4. , Upgrade Program Overview. First, the TA1 platforms will enable hospitals to map their cyber environment and configure a representative simulation of the hospital cyber-environment enabling vulnerability detection and remediation. Second, TA2 will use the map to auto-generate high-fidelity emulators (i.e., "digital twins") of hospital equipment that is prevalent in the hospital network. Third, TA3 will use the emulators and physical samples of hospital equipment (if needed) to rapidly identify vulnerabilities. Fourth, TA4 will take the list of vulnerabilities and develop high-assurance remediations. The remediations are then validated using the TA2 equipment emulators and TA1 simulation of the hospital network to test whether the remediations maintain safety and security guarantees in a realistic network environment. Finally, the TA1 platform gives hospital IT staff the option of automatically deploying the remediations and configuration updates to eliminate vulnerabilities and enhance the security of the network.

Figure 1 - UPGRADE Program Overview



4. PROGRAM-LEVEL REQUIREMENTS

(a) All performers will be responsible for safeguarding information about vulnerabilities whose disclosure may expose healthcare systems to risk. This may involve coordinated vulnerability disclosure amongst affected parties and regulators through appropriate channels.

(b) All performers will achieve all necessary integration & collaboration requirements specified in Figure 2, *Collaboration Requirements*.

(c) Throughout the program, all performers will work with an Independent Verification and Validation (IV&V) team established by ARPA-H. The IV&V team will consist of subject matter experts from the government, Federally Funded Research and Development Centers (FFRDC), academia, and/or other relevant domains. The IV&V team will test and validate technology to confirm performers' progress. Performers will be expected to provide ongoing transparency to the IV&V team and enable detailed, reproducible results during evaluation.

(d) Intellectual Property rights asserted by all proposers are strongly encouraged to be aligned with open-source regimes. Commercially available tools may be leveraged for and/or incorporated into proposed solutions. Licensing details (costs, restrictions, etc.) should align with the

overall goals of the program and should not inhibit collaboration between performers, hospital partners, or the government. (See Section I, Policy Conformation, Agile Development, Software Component Standards, Open Standards, Intellectual Property, and Coordinated Vulnerability Disclosure, for more details)

(e) All performers will develop, and present supplementary metrics (in addition to those specified in Figure 3, UPGRADE Program Metrics) based on their technical approach, enabling the government to measure progress more accurately towards program goals.

(f) All performers will support and attend program events listed in Section H, Schedule, Events, and Deliverables.

(g) All performers will provide deliverables as described in Section H, Schedule, Events, and Deliverables, and their respective TA.

5. TA1 – VULNERABILITY MITIGATION PLATFORM (VMP)

(a) Currently, hospital IT teams are woefully under-resourced and not well equipped to secure the hospital cyber-environment – especially hospital equipment – against cyber-attacks. The objective of TA1 is to create integrated and largely autonomous VMPs that serve as a force-multiplier enabling hospital IT teams to secure vulnerable equipment faster and more effectively. The TA1 platforms will enable non-disruptive rapid characterization and remediation of vulnerabilities to build hospital resilience to cyberattacks and protect the continuity of patient care. The integrated VMPs will be safer and more adaptive, scalable, and tailored, compared to current vulnerability mitigation technologies.

(b) TA1 performers will each work to develop a VMP that supports the following key activities:

- Performer Technology Integration: The tools developed by TA2-4 will be integrated into the VMP to enable under-resourced hospital IT teams to effectively and scalably secure hospital equipment and the larger hospital cyber-environment against cyberattacks that threaten continuity of patient care. The platform will provide access to leading-edge cyber-defense capabilities, irrespective of the size and expertise of the existing hospital IT teams.

- Auto-Mapping of the Cyber-Environment: TA1 will automate the mapping of the complete hospital cyber-environment (including connected hospital equipment and traditional compute devices). This will be automated to the maximum degree possible without risking disruption to hospital operations. The auto-mapping tool will enable TA3 performers to detect vulnerabilities so that TA4 can accelerate the development of remediations.

- Explainable Cyber Decision Support: The VMPs will provide value to multiple hospital stakeholders including, but not limited to, IT teams, leaders of departments that may be impacted by cyber-attacks, and senior hospital administrators. TA1 will be responsible for creating a Cyber Decision Support Tool as part of the platform, which will explain cybersecurity vulnerabilities and mitigation strategies to various non-technical users. This tool will use the vulnerabilities found in TA3 (automated vulnerability detection), and the mitigation solutions developed in TA4 (automated remediation development) as inputs and explain them in plain language as an output. This empowers hospital administrators, who are not expected to be cyber security experts, to make informed decisions about cybersecurity remediations. For example, the platforms will provide IT teams with relevant technical details and tactical recommendations for remediating vulnerabilities, while also providing clinical department leaders with downtime estimates to inform interim mitigation measures. Additionally, the tool could provide a senior hospital administrator with summary information that describes the impact on hospital operations and finances.

- Automated Remediation Deployment: TA1 will automate the deployment of remediations developed by TA4 performers, equipment manufacturers, and software vendors. Examples of deployment approaches include but are not limited to generating a stepwise manual procedure for hospital IT staff or automatically remediating after hospital decision makers concur with a remediation plan (based on actionable information from the cyber-decision support tool).

(c) TA1 will stand up **Whole-Hospital-Simulations (WHS)** that will faithfully recreate representations of the uniquely complex cyber-environments found in hospitals by incorporating physical and digital infrastructure into a mock hospital environment to enable rapid design and testing in a safe,

non-operational setting.

(d) The TA1 WHSs are distinct from the individual TA2 equipment emulators, in that the WHSs focus on replicating the broader hospital cyber-environment, incorporating commercially available virtualization technologies for traditional devices (e.g., laptops, servers, mobile devices) with physical connected hospital equipment, thus mimicking a hospital's real-world configuration. Meanwhile, TA2 will focus on digitally emulating specific classes of hospital equipment that TA1 will progressively incorporate into their WHS to replace physical equipment. The combination of the TA1 WHS and TA2 hospital equipment emulators will enable the creation of a detailed representation of the hospital cyber-environment to accelerate the detection of vulnerabilities (TA3) and enhance the testing of remediations (TA4). Since the WHSs will represent the physical layout and digital configuration of the hospital's cyber-environment, discovered vulnerabilities could be rapidly mapped to the real-world environment for remediation.

(e) TA1 performer(s) will be tasked with integrating technologies developed under TAs 2, 3 and 4 into a comprehensive platform. Each TA1 performer will independently partner with at least one operational hospital to ensure their platform tools are designed around the needs of hospital stakeholders. TA1 performers will be the primary liaison between the UPGRADE program and the hospitals and will be responsible for maintaining a strong understanding of hospital needs, including technical and operational product requirements. TA1 performers will work closely with hospital staff to provide transition training, to ensure developed technologies can continue to be leveraged after the end of the program.

(f) The TA1 integration task will span the full breadth of systems development, from developing requirements and interface documentation, performing system-level design reviews, developing test scripts and scenarios, and orchestrating periodic system level tests and demonstrations. The TA1 performer will use continuous integration/continuous deployment (CI/CD) processes to deliver a functional, living system throughout the program period of performance.

(g) By providing strategies to avoid and mitigate vulnerabilities, the VMP should be designed to bridge the gap between technical complexity and decision-making confidence for users with varying levels of technical expertise. It should significantly enhance hospital decision makers' ability to safeguard and manage critical components of the healthcare

infrastructure, enabling streamlined vulnerability detection-to-remediation within days thereby ensuring U.S. health system resilience against cyberthreats, while improving the quality and continuity of patient care.

6. TA2 – Hospital Equipment Emulation

(a) The objective of TA2 is to create "digital twins" or emulators of hospital equipment that enable deeper understanding of how the equipment behaves and allows for comprehensive cybersecurity testing without risk to operational hospital systems. These digital twins will: serve as components within the digital simulation of the whole hospital cyber-environment (TA1's WHS); accelerate the detection of vulnerabilities (TA3); and enhance the testing of remediations (TA4). TA2 will focus on emulating specific classes of hospital equipment and TA1 will progressively incorporate these emulators into the broader WHSs. Specific classes of equipment of interest are some of the most common, connected, and vulnerable pieces of equipment deployed in hospitals today. These include infusion pumps, patient monitors, IP telephones, imaging equipment, and medication dispensers (see Figure 3, *UPGRADE Program Metrics*).

(b) The primary deliverables of TA2 are emulators of hospital equipment and scalable means to create emulators. Tools and techniques that fully automate emulator development are preferred. These tools will contribute to more robust vulnerability detection, remediation development, testing, and deployment by enabling testing to occur on digital representations of the equipment, instead of operational equipment that is actively being used for patient care.

7. TA3 – Automated Vulnerability Detection

(a) The objective of TA3 is to enable proactive, automatic detection of new and known vulnerabilities across the hospital cyber-environment. How expert hackers discover vulnerabilities remains largely unknown. The tools and high-level strategies have been documented, but without sufficient detail to enable automation of the process. TA3 will study expert hackers as they reason over software and firmware artifacts to create tools and techniques that automate the observed tactics and strategies. This novel approach to vulnerability detection will enable efficient threat detection at scale.

(b) TA3 aims to capture and leverage the thought patterns of expert hackers as they analyze code for vulnerabilities. Using passive, non-invasive biometric sensing, and an instrumented research environment, TA3 will map experts' cognitive states to specific elements (e.g., functions, variables) with minimal disruption to their normal workflow. This process will capture expert intuition about relationships between elements and their vulnerability detection strategies in a comprehensive, machine-readable format. TA3 will develop tools to execute these human expert strategies at machine speed and scale, enabling TA1 to deploy TA4-developed remediations to discovered vulnerabilities faster than adversaries can exploit them.

(c) The primary TA3 deliverables will be automated vulnerability detection tools and models of expert hacker workflows, focused on hospital equipment. These tools will be incorporated into the TA1 VMPs, leveraged by TA4 in the creation of Automated Remediation technology, and will be tested and refined using the WHSs produced by TA1.

(d) TA3 performers are tasked with finding vulnerabilities whose disclosure may expose healthcare systems to risk. TA3 performers will develop and follow strict protocols for coordinated vulnerability disclosure amongst affected parties and regulators through appropriate channels.

8. TA4 – Automated Remediation Development

(a) The objective of TA4 is to automate development and refinement of vulnerability remediation capabilities for known (n-day) and newly detected (0-day) vulnerabilities. TA4 performers will construct models of intended functionality for applications and equipment through analysis of vendor documentation, configuration options, software/firmware artifacts, patterns of clinical use, and network environment details. When a vulnerability is discovered in a system, TA4 will use these models to inform the development/selection of an appropriate remedy. Potential remedies may include but are not limited to vendor-provided remediations, application/equipment configuration changes, network architecture changes, network traffic modification, and input filtering.

(b) As the program continues, these defensive capabilities will be thoroughly tested in TA2's emulated hospital equipment and as part of the WHSs developed by TA1. This will allow TA4 performers to validate the efficacy of the remediation and ensure that the functionality of other connected equipment is not negatively impacted. TA4 tools will receive actionable

vulnerability information from TA3 scanning tools. Any vulnerabilities that are unable to be automatically mitigated will be prioritized for manual review along with all pertinent information regarding the threat and possible mitigations.

(c) TA4 will test their remediations in the WHSs to identify optimal deployment pathways, however, TA1 will develop the technology to autonomously deploy the remediations in the operational hospital environment. Ultimately, TA4 will enable streamlined detection-to-remediation within 5 days or faster, representing a significant reduction in the defensive capability development and deployment timeline.

(d) The primary deliverables for TA4 will be tools for automated development of models of intended functionality and vulnerability remediation capabilities for hospital equipment classes of interest (see Equipment Classes in Figure 3, *UPGRADE Program Metrics*).

F. PROGRAM STRUCTURE AND INTEGRATION

1. All TA2, TA3, and/or TA4 performers are expected to collaborate with all TA1 performers. To minimize risk and manage integration between Phases, progression to Phase II will depend on performance against Phase I metrics (Figure 3, UPGRADE Program Metrics) and milestones (Figure 4, *UPGRADE Schedule and Milestones*).

2. Multiple awards are anticipated for TA1 to ensure applicability of platforms to different hospitals. To foster a diversity of solutions, multiple performers are expected to be selected for TA2, TA3, and TA4. Collaboration between multiple types of organizations, academic institutions, and commercial companies is highly encouraged. Collaboration expectations are described in the **Error! Reference source not found.**, *Collaboration Requirements*. Please note collaboration between TAs is expected and is necessary to meet the objectives of the UPGRADE program (see Section K, *Performer Collaboration/Associate Contractor Agreement*).

Figure 2. Collaboration Requirements

TA	Collaboration Expectations
All	All TA performers, 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.

	All TA performers, in collaboration with ARPA-H, will align on technical standards for all TAs (e.g., common data standards, formats, and specifications) to enable consistency and accessibility across all performers. Performers will also lay the foundation to enable platform extensibility after the end of the program.
TA1	**With TA1:** Coordinate programmatic events with ARPA-H personnel and other TA1 performers to avoid scheduling and resource conflicts.
	With TA2: TA1 performers should collaborate with TA2 performers to integrate the emulated hospital equipment into their WHS and VMP. TA1 performers should provide TA2 performers with access to the outputs from the cyber-environment mapping tool, access to their VMP, and access to their WHS for testing purposes.
	With TA3: TA1 performers should collaborate with TA3 performers to include the vulnerability detection tools into their WHS and VMP. TA1 performers should work with TA3 performers to ensure the severity and description of the vulnerabilities are accurately reflected in the Explainable Cyber Decision Support Tool. TA1 performers should provide TA3 performers with access to the outputs from the cyber-environment mapping tool, and access to their VMP and WHS for testing purposes.
	With TA4: TA1 performers should collaborate with TA4 performers to integrate the remediation tools into their WHS and VMP. TA1 performers should work with TA4 performers to ensure the remediations are accurately described in the Explainable Cyber Decision Support Tool and ensure that developed remediations are viable for deployment in an operational hospital environment. TA1 performers should provide TA4 performers with access to the outputs from the cyber-environment mapping tool, and access to their VMP and WHS for testing purposes.
TA2	**With TA1:** TA2 should collaborate with TA1 to integrate the emulated hospital equipment into the WHSs and the VMPs. TA2 performers should coordinate with TA1 to receive access to the outputs from the cyber-environment mapping tools, and access to the VMPs and WHSs for testing connectivity and behavior of the emulators within the WHS.
	With TA3: TA2 performers should share the complete emulators of the hospital equipment to enable TA3 performers to develop technologies to detect vulnerabilities. TA2 should coordinate with TA3 by allowing for a review of the initial hospital equipment emulation and soliciting feedback necessary for TA3 to complete their deliverables.
	With TA4: TA2 performers should share the complete emulators of the hospital equipment that will allow TA4 performers to develop technologies to remediate vulnerabilities.
TA3	**With TA1:** TA3 should collaborate with TA1 to include their vulnerability detection tools into the WHSs and on the VMPs. TA3 performers should work with TA1 performers to ensure the severity and description of the vulnerabilities are accurately reflected in the TA1 Explainable Cyber Decision Support Tool. TA3 performers should 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.
	With TA2: TA3 should coordinate with TA2 by reviewing initial hospital equipment emulators and providing feedback necessary for the completion of TA3 deliverables. TA3 should collaborate with TA2 to ensure vulnerability detection tools function appropriately on TA2 emulators.

	With TA4: TA3 performers should work with TA4 performers to ensure that information about auto detected vulnerabilities (TA3) is effectively passed along to be used in the development of remediations for those vulnerabilities (TA4)
TA4	With TA1: TA4 performers should collaborate with TA1 performers to include the remediation tools into the WHSs and on the VMPs. TA4 performers should work with TA1 performers to 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. TA4 performers should receive from TA1 performers access to the outputs from the cyber-environment mapping tool, and access to their VMP and WHS for testing purposes.
	With TA2: TA4 performers should receive complete emulators from TA2 performers, enabling TA4 performers to develop technologies to remediate vulnerabilities.
	With TA3: TA4 performers should share remediation outputs with TA3 to refine work product and technologies.

G. PROGRAM METRICS

Metrics for each phase of the four TAs are outlined in the Error! Reference source not found.:

Figure 3: UPGRADE Program metrics.

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%

H. SCHEDULE, EVENTS, AND DELIVERABLES

1. SCHEDULE

(a) UPGRADE is a three-year, two-phase program that consists of four interconnected TAs. Phase I (Base period) spans months zero to 18 and Phase II (Option 1) spans months 19 to 36.

(b) Options may be exercised at the government's sole discretion, based on technical progress measured against the program metrics, milestones, and funding availability (see Figure 3, *UPGRADE Program Metrics*, and Figure 4, *UPGRADE Schedule and Milestones*).

(c) Technical progress towards the metrics of the program is a significant deciding factor for continuation into subsequent phases and will be monitored through the management and program events depicted in the following paragraph.

2. MANAGEMENT- AND PROGRAM EVENTS: The government will specify the locations for all program events, which are described below.

(a) Monthly virtual team meetings with additional virtual/hybrid/in-person meetings as needed.

(b) Site visits, up to two per phase, where the ARPA-H team will meet with at performer site(s). During these visits, the ARPA-H team will assess progress towards program goals via performer briefings, technical discussions, demonstrations, and informal end-of-phase evaluations/challenges. Members of the IV&V team may join ARPA-H for these visits.

(c) Kickoff meetings at the beginning of each phase to jumpstart research and development efforts and collaboration across all performers. The kickoff meeting will focus on open technical exchange, discussion of the research problems encompassed by the UPGRADE program, and how effective cross-discipline collaboration may address these research problems. The government will specify the location for the phase kickoff meetings. For budgeting purposes, assume the kickoff meeting will take place in Arlington, VA, run for three days, and include most of each team's personnel.

(d) Hackathons to focus on open, technical exchange that includes

discussion of difficulties encountered and possible solutions. The goals of the hackathons will be to:

(1) Review and share innovations/accomplishments of the program;

(2) Review and discuss plans and options for technology demonstrations and prototypes;

(3) Review and discuss results from meetings and events conducted prior to the tests and evaluations;

(4) Demonstrate prototypes; and

(5) Plan for the following evaluation. There will be three (3) hackathons in each phase, starting at four months (see Figure 4, UPGRADE Schedule and Milestones).

The government will specify the location for the hackathons. For budgeting purposes, assume the hackathons will alternate between San Francisco, CA and Boston, MA, run for 3.5 days, and include most of each team's personnel.

(e) Evaluation events at the end of each phase to test the integrated TA1 systems and demonstrate the capabilities of TA2, TA3, and TA4 individually with the IV&V team and ARPA-H. The government will specify the location for evaluation events. For budgeting purposes, assume the kickoff meeting will take place in Arlington, VA, run for four days, and include most of each team's personnel.

3. KEY MANAGEMENT- AND PROGRAM DELIVERABLES

(a) System Development Plan (SDP). An SDP will be provided within one month after the kickoff meeting for each phase and shared with other performers for synchronization. The SDPs for each phase will be based on the performers' proposed technical solution and will be presented at the kickoff meeting for each phase. The SDP will describe the scope of the design and development effort, describe the hardware and software architecture in sufficient detail for review and planning, reference any applicable documents, and provide a program schedule.

(b) Edge of the Art (EotA) Report. EotA reports discussing the existing tools

and techniques available for respective technical areas and the applicability or lack thereof (i.e. limitations) to the hospital equipment classes of interest to the UPGRADE program. These reports should involve detailed analysis of the strengths and weaknesses of each technology/tool considered by performers for their TA(s). These reports will be due three months into each phase, with an update provided 12 months into each phase. These reports should not include proprietary information and may be shared with other government partners.

(c) Software and Software Documentation

(1) All computer software developed or delivered under the UPGRADE program should be delivered as source and as object (executable) code. The source listings and source code for the target computer systems, as well as any build scripts or other technical information required for ARPA-H to compile all delivered source code should be included. Also see Section I Policy Conformation, Agile Development, Software Component Standards, Open Standards, Intellectual Property, and Coordinated Vulnerability Disclosure, paragraph (3) for Intellectual Property right details associated with program deliverables.

(2) Delivered software under this effort is to be completely maintainable and modifiable with no reliance on any non-delivered computer programs or documentation. Permission from the ARPA-H Program Manager and Agreements Officer is required if commercially licensed software is part of these deliverables. Software documentation should document source code, system diagrams, part numbers and other data necessary to maintain and to produce copies of the software.

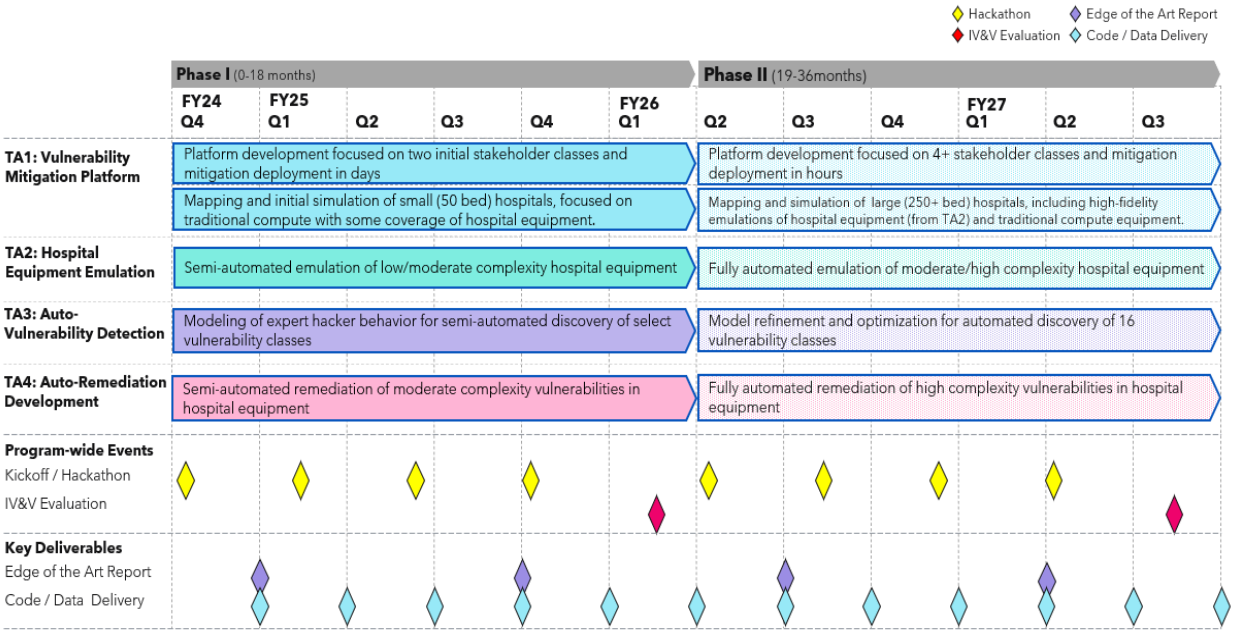
(d) Quarterly technical and financial status reports that will be discussed with the ARPA-H team.

(e) A final phase report for each program phase that concisely summarizes the effort conducted, technical achievements, and remaining technical challenges will be due thirty days after the end of each phase.

(f) A final technical report at the end of the overall period of performance that summarizes the performer's effort.

(g) ARPA-H may request performer data as deemed necessary throughout the program to validate technical progress.

Figure 4: UPGRADE Schedule and Milestones



I. POLICY CONFORMANCE, AGILE DEVELOPMENT, SOFTWARE COMPONENT STANDARDS, OPEN STANDARDS, INTELLECTUAL PROPERTY, AND COORDINATED VULNERABILITY DISCLOSURE

1. POLICY CONFORMANCE

(a) Proposers are expected to adhere to all relevant laws and policies applicable to data and information systems and technologies, including but not limited to:

- Common IT Security Configurations,
- Federal information technology directives and policies,
- Section 508 of the Rehabilitation Act of 1973 (29 USC 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998), and
- HHS OCIO Policy for Information Technology (IT) Enterprise Performance Life Cycle (EPLC)
- The appropriate coordinated vulnerability disclosure guidance for sharing critical information with relevant stakeholders. (e.g., https://www.cisa.gov/coordinated-vulnerability-disclosure-process)

(b) All proposed research is expected to be unclassified.

(c) HHS has released a set of voluntary Cybersecurity Performance Goals (CPGs)[20] to assist with prioritization of high-impact cybersecurity improvements. UPGRADE performers should indicate the CPGs, both "essential" and "enhanced" that their approaches address.

(d) In concert with ARPA-H, proposers should address innovative solutions to design, architect, develop, test, and implement tools and associated open standards as described in the TAs. It is expected that all performers will work together to converge on standards and APIs to ensure interoperability across prototype capabilities. All performers are expected to follow agile software development processes.

2. SOFTWARE COMPONENT STANDARDS

(a) The healthcare data eco-system is complex and multi-dimensional with a variety of standards for data models, data transmission protocols, data routing methods etc. that are similar to and extend the International Standards Organization (ISO) Open Systems Interconnection Model (OSI)[21]. ARPA-H programs are likely to involve research that touches on multiple layers of the OSI model from low level radio frequency (RF) based protocols for transmission of data from implantable devices (potentially OSI layers 1-5), to secure and fault tolerant networking protocols for medical devices (potentially OSI layers 3-6) to the exchange of health information including Electronic Health Records, lab results and medical images related to a patient between healthcare facilities and health data brokers including but not limited to Health Information Exchanges (HIE) and Trusted Exchange Framework and Common Agreement (TEFCA) Qualified Health Information Networks using protocols such as HL7 FHIR (OSI Layer 7). This diversity requires careful consideration of the most appropriate standards to be used for the specific technologies in development and the layer at which they operate.

(b) ARPA-H is committed to advancing interoperability in today's health ecosystem through the adoption of open, consensus driven standards and laying the foundation for emerging technologies to interoperate in the health ecosystem of the future through the evolution of these standards across all layers of the health data IT eco-system. With that in mind, we anticipate that potential performers will develop software and data communication components that fall into three categories:

- components that can leverage today's existing standards without impeding the R&D,
- components where extensions to existing standards will be necessary to unlock new capabilities in an interoperable way, and
- components in areas where consensus-based standards do not yet exist or where use of standards would seriously limit the ability to efficiently conduct R&D.

(c) Whenever such an existing standard is available that meets the scientific, technical, and research needs of the proposed effort, performers must use the existing standard instead of creating their own. In cases where an existing standard provides only partial functionality, performers should expand upon the existing standard, ideally in a way that does not prohibit or interfere with backward compatibility, and create sufficient documentation for Office of the National Coordinator for Health Information Technology (ONC), the U.S. Department of Health and Human Services (HHS) agencies or standards organizations, to evaluate extensions for potential inclusion in the standard (including open Application Programming Interfaces (APIs) and open data formats).

(d) In the case of information relating health and healthcare data at higher layers of the OSI model, all health information technology (IT) components should adhere to or (as needed) expand upon applicable national standards adopted by HHS, including the ONC (e.g., Fast Healthcare Interoperability Resources (FHIR) and United States Core Data for Interoperability (USCDI)).[22]

(e) Technical solutions that contain software elements, commercial-friendly open-source licenses (e.g., MIT, BSD, or Apache 2.0) are preferred.

(f) Adhering to international standard ISO/IEEE 11073 will enable broad support for current and future devices, especially those developed internationally. At other layers of the OSI model, and for software components operating outside the network stack (e.g. health databases, Picture Archiving and Communication Systems (PACS) etc.), other standards will be relevant and technical solutions should seek to utilize or expand upon appropriate open, consensus-based standards[23].

(g) If a technical solution requires an extension of existing standards or development of technologies outside of the standards, the proposer must schedule a meeting with ARPA-H representatives to discuss the

deviation to the standards prior to proposal submission.

3. OPEN STANDARDS/INTELLECTUAL PROPERTY

(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. A key goal of the project is to seed the establishment of a sustainable open-source ecosystem for automated vulnerability detection and remediation. Thus, it is desired that all non-commercial software (including source code), software documentation, and technical data generated by the project, be provided as deliverables to the government with open-source or unlimited rights, and all hardware designs and documentation be provided with a minimum of government Purpose Rights (GPR), as lesser rights may negatively impact the potential for this health IT ecosystem to become self-sustaining. Open-source code is highly encouraged using permissive, business-friendly open-source licenses such as CC-BY, BSD, MIT, Apache 2.0, or similar. Approaches that inhibit this objective are not desired and would adversely affect the UPGRADE program goals and objectives.

(b) Performers will develop and follow strict protocols for coordinated vulnerability disclosure amongst affected parties and regulators through appropriate channels.

J. ELECTRONIC INVOICING AND PAYMENTS

Performers will be required to register in and to submit invoices for payment directly to Payment Management Services (PMS) unless an exception applies.

K. PERFORMER COLLABORATION/ASSOCIATE CONTRACTOR AGREEMENT (ACA)

1. The ARPA-H UPGRADE program will be comprised of performers that include contractors and subcontractors, to include those with deep knowledge of key data assets as well as those selected through this announcement or through complementary funding mechanisms at partner organizations. Therefore, it is expected that performers will interact and work collaboratively with other performers.

2. To facilitate the open exchange of information described above, performers will

have Associate Contractor Agreement (ACA) language included in their award. Each performer will work with other UPGRADE performers to develop an ACA that specifies the types of information that will be freely shared across performer teams. The expected collaboration requirements are described in detail in Figure 2. Collaboration Requirements.

3. It is intended that ACAs are established, after award, but prior to the first hackathon in month 4 of Phase I between TA performers (see Figure 2, Collaboration Requirements). The open exchange of scientific information will be critical in advancing the software research required to achieve the UPGRADE objectives. The ACA will establish a common understanding of expectations to guide the open exchange of ideas and establish a collaborative foundation for the UPGRADE project.

L. AWARD INFORMATION

1. Multiple awards are anticipated under this announcement; however, the number of proposals selected for award will depend on the quality of the proposals received and the availability of funds. Proposals selected for award negotiations will result in an award under an Other Transaction (OT) type contract agreement.

2. See Section 1.4 of the MAI, ARPA-H-MAI-24-01 (through Amendment 01) for additional information on award information.

M. ELIGIBILITY

See Section 2 of the MAI, ARPA-H-MAI-24-01 (through Amendment 01) for eligibility requirements.

N. MODULE ANNOUNCEMENT RESPONSES

1. SOLUTION SUMMARY CONTENT AND FORMATTING. Submission of a Solution Summary is a mechanism for potential proposers to get feedback prior to investing resources for a full proposal. All Solution Summaries submitted in response to this Module Announcement must comply with the content, page, and formatting requirements in Appendix A. Potential proposers are strongly encouraged to use the template provided. Information not explicitly requested in this Module Announcement may not be reviewed.

   NOTE: no awards will be made, nor funding provided as a result of Solution

Summary submissions.

2. SOLUTION SUMMARY SUBMISSIONS

Solution Summaries shall be submitted to the ARPA-H Solution Site https://solutions.arpa-h.gov/ by **10:00 PM ET on July 22, 2024**. Solution Summaries received after this date or submitted incorrectly (e.g. not submitted to the ARPA-H Solutions Site by the due date and time) may not be reviewed.

3. SOLUTION SUMMARY FEEDBACK

ARPA-H will provide written feedback to all Solution Summary submissions. Feedback at a minimum will provide an encourage or discourage recommendation in submitting a proposal to the ARPA-H UPGRADE Module Announcement. Feedback will be sent to the administrative and technical points of contact noted on the Solution Summary cover page.

NOTE: All parties, whether encouraged or discouraged to submit a proposal, are eligible to submit a proposal to the ARPA-H UPGRADE Module Announcement.

4. COMMUNICATIONS.

Communication beyond the written Solution Summary feedback will be limited to the ARPA-H Module Announcement Questions and Answer (Q&A) process.

NOTE: ARPA-H cannot dictate solutions or transfer technology.

O. PROPOSAL CONTENT AND FORMAT

This Module Announcement is soliciting Stage 1, Volume 1 proposals. Stage 1 Volume 1 proposals should contain the following document submissions (see Attachment 1, OT Bundle which provides templates for the Stage 1, Volume 1 proposals):

1. TECHNICAL & MANAGEMENT

(a) All submissions, including proposals, must be written in English. Below is the page restriction for each Module category. If proposing to multiple TAs, the proposer should submit a combined proposal and choose a module category commensurate with the proposed technical solution:

- **BIT Module** is ≤ $2,000,000: Volume 1 should be limited to **15** pages.
- **BYTE Module** is > $2,000,000 ≤ $5,000,000: Volume 1 should be limited to **20** pages.
- **KILO Module** is > $5,000,000 ≤ $10,000,000: Volume 1 should be limited to **25** pages.
- **MEGA Module** is > 10,000,000 ≤ $25,000,000; Volume 1 should

be limited to 30 pages.

- GIG Module is > $25,000,000 ≤ $50,000,000; Volume 1 should be limited to 35 pages.

Page restrictions apply ONLY to the Technical & Management section Stage 1, Volume 1 submission.

NOTE: Proposals should select a cost point that is commensurate with the scale and complexity of the proposed approach. Proposals that simply align a proposed budget to the Module Category ceiling value stated above are strongly discouraged. Thus, if a proposal is selected for Stage 2 submissions and the basis of estimate was simply aligned to the Module Category ceiling value, the government will require a full cost proposal (i.e., direct and indirect rates, labor hours, equipment, material, other direct costs, etc.) that should be substantiated by salary documentation, indirect rate agreements, material and equipment quotations and a justification for proposed labor categories and hours that correlates directly to the proposed Task Description Document. The submission of a full cost volume will impact Stage 2 price/cost proposal timelines and will likely be followed by extensive cost negotiations.

(b) All proposers, regardless of TA, should address the following Program-Level Requirements in their proposals:

(1) All performers will be responsible for safeguarding information about vulnerabilities whose disclosure may expose healthcare systems to risk. This may involve coordinated vulnerability disclosure amongst affected parties and regulators through appropriate channels.

(2) All performers will achieve all necessary integration & collaboration requirements specified in Figure 2, Collaboration Requirements.

(3) Throughout the program, all performers will work with an Independent Verification and Validation (IV&V) team established by ARPA-H. The IV&V team will consist of subject matter experts from the government, Federally Funded Research and Development Centers (FFRDC), academia, and/or other relevant domains. The IV&V team will test and validate technology to confirm performers' progress. Performers will be expected to provide ongoing transparency to the IV&V team and enable

detailed, reproducible results during evaluation.

(4) Intellectual Property rights asserted by all proposers are strongly encouraged to be aligned with open-source regimes. Commercially available tools may be leveraged for and/or incorporated into proposed solutions. Licensing details (costs, restrictions, etc.) should align with the overall goals of the program and should not inhibit collaboration between performers, hospital partners, or the government. (See Section I, Policy Conformance, Agile Development, Software Component Standards, Open Standards, Intellectual Property, and Coordinated Vulnerability Disclosure, for more details)

(5) All performers will develop, and present supplementary metrics (in addition to those specified in Figure 3, *UPGRADE Program Metrics*) based on their technical approach, enabling the government to measure progress more accurately towards program goals.

(6) All performers will support and attend program events listed in Section H, Schedule, Events, and Deliverables.

(7) All performers will provide deliverables as described in Section F and their respective TAs.

(c) TA1 proposals should address the following topics:

(1) All Program-Level Requirements (see Section O(1)(b).

(2) TA1 performers will individually and independently partner with at least one hospital or hospital system over the course of the program. Identification of specific hospital partner(s) is highly encouraged and preferred at the proposal stage. Proposals should include a letter of support or similar sign of commitment from a hospital stakeholder. At a minimum, the specific hospital partnership(s) should be well defined as early as possible in Phase I. TA1 performers are encouraged to partner with critical-access and under-resourced hospitals to demonstrate the benefits of the VMP in high-risk settings. Additional partner hospitals may be added or replaced during the life of the program, with government approval.

(3) TA1 performers will work closely with hospital partners to minimize and manage risk to the operational hospital environment across all activities. TA1 proposals should describe how the proposed work will be conducted to minimize and manage risk to hospital operations.

(4) TA1 performers will automate the mapping of hospital networks and deployed equipment in a comprehensive manner, without disrupting hospital operations. Common techniques (e.g., active scanning) may require modification to be safely and effectively used. Proposals should consider sources of information beyond network traffic data and how these sources might be integrated without manual effort.

(5) TA1 will provide a range of technical, clinical, and administrative stakeholders with appropriate explanations on cyber issues in their environment. This information should be provided via workflows that fit the needs and obligations of each stakeholder role. Proposals should enable interactive exploration of the presented information as well as discuss the composability of underlying data and models.

(6) TA1 will enable automated deployment of a variety of remediation and mitigation capabilities into the hospital cyber-environment. Proposals should automate the use of existing equipment / application features and management interfaces rather than requiring endpoint-based agents (e.g., SolarWinds) or generating stepwise manual procedures for hospital staff.

(7) TA1 performers will develop their VMPs as flexible frameworks that can integrate mature commercial technologies alongside performer-developed prototypes. Proposals should orchestrate the use of existing technology in hospital cyber-environments rather than replace them by default.

(8) TA1 performers will demonstrate that their VMPs are able to be effectively utilized by small, under-resourced IT teams. This may involve onsite deployment and training and working with hospital IT staff to ensure familiarity with VMP usage that enables continued usage beyond the duration of the UPGRADE program. Proposals should demonstrate scalability as resource levels and representative technical challenges change.

(9) TA1 performers will simulate the complex cyber-environments found in hospitals by incorporating physical and digital infrastructure into a mock hospital environment to enable rapid design and testing in a safe, non-operational setting. This WHS may incorporate a combination of commercial and open-source virtualization technology, TA2-developed emulators, vendor provided software, and physical equipment. Proposals should minimize the use of physical equipment over the course of the program while still providing a high-fidelity simulation environment.

(10) TA1 performers will conduct regular red team exercises against simulated hospital cyber-environments as part of the WHS development process to demonstrate progress and overall viability of the proposed approach. Proposals should use these exercises to produce useful data on the performance of existing commercial tools and identify potential gaps for the VMS to address. This will ensure UPGRADE is measured against a baseline that always represents the current state of practice.

(11) TA1 performers will use industry best practices (e.g., user-centered design) for user interface/user experience (UI/UX) development, as appropriate. Proposals should capture current stakeholder practices and develop mental models for each one's role in protecting patients by securing the hospital cyber-environment as part of interface development.

(12) TA1 proposals should present a clear integration and relationship management plan across all necessary stakeholders including all TA performers, hospitals partners, and the government.

(13) TA1 performers will collaboratively align on common data formats and application programming interfaces (APIs) to enable data sharing and data integration with performers and stakeholders as appropriate.

(14) TA1 performers will present a long-term sustainment strategy for their VMP and WHS. Proposals will present commercialization strategies that minimize healthcare provider costs while enabling future innovation.

(15) The following are out of scope for TA1 proposals: Solutions that focus exclusively on traditional compute rather than connected hospital equipment.

(d) TA2 proposals should address the following topics:

(1) All Program Level Requirements (see Section O(1)(b).

(2) TA2 performers will endeavor to develop hospital equipment emulators that can be scaled based on available compute resources. Existing virtualization technologies (e.g., QEMU) may be used as part of this process. TA2 performers may use any artifacts that can be retrieved from the equipment including but not limited to firmware and configuration files. Performers may also use publicly available source code for software associated with equipment of interest. Thus, proposals should consider a variety of equipment-related artifacts and approaches to characterizing equipment behavior.

(3) TA2 performers may use non-public artifacts (e.g., manufacturer provided, previously developed) if they are legally permitted to do so. Proposals intending to use non-public, manufacturer-provided artifacts should include a letter of support from at least one equipment manufacturer indicating their willingness to partner in support of program objectives.

(4) TA2 performers will develop tools to automate and accelerate the rate at which newly encountered equipment may be emulated. Proposals should break down the steps involved (e.g., reverse engineering, rehosting, validation) and clearly identify how the proposed approach impacts each one. Proposals should also seek to fully automate the emulator development process.

(5) TA2 performers will leverage models of common sub-components (e.g., FPGAs, ASICs, microcontrollers) across different equipment, instead of recreating each emulator from the ground-up. Proposals should explain how platform and/or architecture agnostic approaches for equipment emulation will be developed.

(6) TA2 performers will develop emulators with sufficient fidelity and performance to interact with external equipment and applications,

enable vulnerability discovery, and validate applied remediations. Proposals should explain how potential impacts to equipment behavior based on TA1-deployed remediations will be characterized.

(7) TA2 performers will focus on emulating at least one hospital equipment class of interest during each phase of the program as specified in the TA2 metrics (see Figure 3, UPGRADE Program Metrics). Proposals should clearly explain how all classes of the hospital equipment specified in the TA2 metrics will be emulated.

(8) TA2 performers will develop approaches that provide evidence as to emulator fidelity with minimal use of hardware-in-the-loop. Proposals should clearly describe the proposed approaches.

(9) The following features are out of scope for TA2 proposals:

(i) Approaches relying exclusively on physical equipment for analysis.
(ii) Solutions that focus on traditional compute rather than connected hospital equipment.

(e) TA3 proposals should address the following topics:

(1) All Program Level Requirements (see Section O(1)(b).

(2) TA3 performers will study the behavior and workflows of expert hackers as they search for vulnerabilities and will create predictive models based on these observations. This may involve a combination of active and passive instrumentation including but not limited to gaze tracking, electroencephalography (EEG), system monitoring, and interviews. Proposals should describe the approach for studying expert hacker behavior and workflows.

(3) TA3 performers will limit expert hackers under observation to analysis of artifacts that can be reasonably acquired (e.g., application binaries, firmware images) or are publicly available (e.g., open-source code). Proposals should describe the artifacts that will be utilized.

(4) TA3 performers will recruit experienced individuals from the hacker community that have proven experience finding multiple

0-day vulnerabilities in applications and devices with similar features to the connected hospital equipment classes of interest. Proposals should describe the approach to recruiting these experienced hackers.

(5) TA3 performers aim to develop automated vulnerability detection tools and techniques based on the models of expert hacker behavior. These tools need to produce an automated means of exercising a discovered vulnerability, or a proof of vulnerability (PoV). This will ensure that discovered vulnerabilities are not false positives and assist TA1 and TA4 with verification of successful remediation. Proposals should describe the approach to developing automated vulnerability detection tools.

(6) TA3 performers will develop tools that are applicable to at least one common platform and architecture combination (e.g., Linux on ARM) in the hospital equipment classes of interest to TA2. (see Figure 3, *UPGRADE Program Metrics*) TA3 performers will provide a path forward to development and testing using available artifacts (e.g., firmware) as TA2-developed emulators will not be available at the beginning of the program. Proposals should pursue platform and/or architecture agnostic approaches for detecting vulnerabilities across multiple hospital equipment classes of interest.

(7) TA3 performers may use non-public artifacts (e.g., manufacturer provided, previously developed) to develop vulnerability detection tools, if they are legally permitted to do so. Proposals intending to use non-public, manufacturer-provided artifacts should include a letter of support from at least one equipment manufacturer indicating their willingness to partner in support of program objectives.

(8) TA3 performers will need to address multiple vulnerability classes or Comment Weakness Enumerations (CWEs) in each phase of the program (see Figure 3, *UPGRADE Program Metrics*) and discuss why detecting the selected classes will have significant positive impact on the cybersecurity of at-risk hospitals. Proposals should address more classes of vulnerability per phase than required by the TA3 metrics.

(9) TA3 performers will develop touchpoints to direct vulnerability

discovery analyses based on the state of the hospital cyber-environment. Proposals should detect vulnerabilities that involve context from multiple pieces of equipment, applications, and/or the network environment.

(10) The following features are out of scope for TA3 proposals:

(i) Solutions that focus on traditional compute rather than connected hospital equipment.
(ii) Vulnerability detection techniques that are largely manual.

(f) TA4 proposals should address the following topics:

(1) All Program Level Requirements.

(2) TA4 performers will produce high-fidelity models of intended behavior for applications and hospital equipment with minimal manual effort. TA4 proposals should describe the approach to producing these high-fidelity models.

(3) TA4 performers will develop remediation capabilities across at least one class of hospital equipment per phase. TA4 proposals should develop targeted remediations that specifically address given vulnerabilities rather than generalized defenses.

(4) TA4 performers will develop tools to automate and accelerate the rate at which new remediation and mitigation capabilities can be developed. TA4 proposals should describe these tools that will be developed.

(5) TA4 performers will develop remediation development capabilities that are applicable to at least one common platform and architecture combination (e.g., Linux on ARM) in the hospital equipment classes of interest to TA2. TA4 proposals should develop platform and/or architecture agnostic approaches to vulnerability remediation that could be applied to all hospital equipment classes of interest.

(6) TA4 performers will consider vendor provided resources (e.g., remediations, recommended configurations) in addition to novel, TA4-developed options. Proposals should leverage resources and products that are open-source and/or support cross-vendor

integration.

(7) TA4 performers may use non-public artifacts (e.g., manufacturer provided, previously developed) to develop vulnerability detection tools, if they are legally permitted to do so. Proposals intending to use non-public, manufacturer-provided artifacts should include a letter of support from at least one equipment manufacturer indicating their willingness to partner in support of program objectives.

(8) TA4 performers will develop vulnerability remediation capabilities that do not interfere with the intended functionality of defended hospital equipment or applications. TA4 proposals should describe how they will manage risk and not interfere with hospital equipment or applications.

(9) TA4 performers will prioritize automating the use of existing equipment/application features and management interfaces for vulnerability remediation rather than deploying endpoint-based solutions. TA4 proposals shall describe their approach to meeting this objective.

(10) The following features are out of scope for TA4 proposals:

(i) Solutions that focus on traditional compute rather than connected hospital equipment.
(ii) Remediation development technologies that are largely manual.

(g) Software Component Standards

(1) Technical solutions that contain software elements, commercial-friendly open-source licenses (e.g., MIT, BSD, or Apache 2.0) are preferred. If an open, consensus-based standard does not yet exist, proposers should identify the aspects that lack an open standard, describe a plan to develop a general-purpose open data model and to prototype new open APIs. Proposals should explain how the performer will enhance data interoperability (including semantic interoperability) and expand the availability of open, consensus-based standards and data models.

(2) Proposals must include a technical plan to align with applicable

standards based on the OSI layer at which they are operating including but not limited to HHS-adopted health IT standards (45 CFR Part 170 Subpart B). For the full description of standards adopted in CFR Part 170, Subpart B, please review the complete text of the regulations when applicable, technical solutions should also outline integration with the Trusted Exchange Framework and Common Agreement (TEFCA).

(h) Data Storage and Analysis Costs. Proposers should provide details surrounding data storage and analysis cost estimates; however, these cost assumptions should not be included in the total Basis of Estimate costs, as these will be covered by the UPGRADE program and provided as a Government Furnished Resource. If proposers anticipate that government-provided cloud resources will not be sufficient, proposers should provide justification within the Stage I, Volume I proposal submission regarding why they will be leveraging their own resources.

(i) Equity Requirements

(1) ARPA-H is committed to equitable health care access irrespective of race, ethnicity, gender/gender identity, sexual orientation, disability, geography, employment, insurance, and socioeconomic status. Accordingly, all proposals should include an equity and accessibility plan outlined in the Bundle of Attachments, Volume 1 Technical & Management.

(2) The UPGRADE Program aims to improve health equity across the United States by vastly improving hospital cybersecurity, especially for under-resourced facilities. Without the need for costly measures to prevent and manage cyber-attacks, resources can be reallocated to enhance patient care. UPGRADE wishes to ensure that hospitals and clinics from diverse geographic locations are included, especially those in rural and underserved urban areas. These locations often have different resource constraints and may face unique cybersecurity challenges. Performers will partner with hospital IT staff, consultants, healthcare providers, and administrators to develop solutions that are scalable and adaptable to different levels of existing infrastructure and resources. At the outset and ongoing during the program, UPGRADE will develop clear and transparent policies about data usage as well as engage with community representatives to build trust. During program reviews, ARPA-H

will assess whether the program inadvertently favors certain types of hospital equipment or technologies that might not be uniformly available across different hospitals.

(3) The UPGRADE Program's solutions will elevate cybersecurity standards universally without widening the technology gap between different health care facilities. UPGRADE aims to reduce the need for high-level expertise to implement effective cybersecurity by automating and accelerating responses to cyber threats. Therefore, UPGRADE solutions will be usable with only a moderate amount of cybersecurity training. This will help ensure an enhanced cybersecurity capacity is available to clinics and hospitals across the U.S. independent of the size or location of the facility.

2. BASIS OF ESTIMATE (BOE)

3. TASK DESCRIPTION DOCUMENT (TDD)

4. ADMINISTRATIVE AND NATIONAL POLICY REQUIREMENTS

NOTE: Section 5.2 of the MAI, ARPA-H-MAI-24-01 (through Amendment 01) provides information on Administrative and National Policy Requirements that may be applicable for proposal submission as well as performance under an award.

P. PROPOSAL SUBMISSION INSTRUCTIONS

1. 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.

2. All proposals submitted in response to this announcement should comply with the content and formatting requirements of the OT Bundle (see Attachment 1). Proposers should use the templates provided in the OT Bundle associated with this announcement. Information not explicitly requested in the MAI, this announcement, or OT Bundle may not be evaluated.

3. All proposal submissions shall be submitted to https://solutions.arpa-h.gov/, ensuring receipt by the government by date and time specified in paragraph 1 of Section Q, Proposal Due Date and Time, of this Module Announcement. **Proposals must be submitted ONLY to the ARPA-H Solutions portal**. Proposals

submitted to the electronic Contract Proposal Submission (eCPS) will NOT be reviewed.

Q. PROPOSAL DUE DATE AND TIME

1. Proposals in response to this notice are **due no later than 12:00 PM ET on September 18, 2024**. Full proposal packages as described in Section O, *Proposal Content and Format*, must be submitted per the instructions outlined in this Module Announcement and received by ARPA-H no later than the above time and date. Proposals received after this time and date will NOT be reviewed.

2. Proposers should consider the submission time zone (Eastern Time) and that some parts of the submission process may take from one business day to one month to complete (e.g., registering for a Unique Entity Identifier (UEI) number through SAM.gov, or Tax Identification Number (TIN); see Section 5.2.1 of the MAI (through Amendment 01) for information on obtaining a UEI and TIN).

R. PROPOSAL EVALUATION AND SELECTION

Proposals selected and evaluated in accordance with Section 4 of the MAI, ARPA-H-MAI-24-01 (through Amendment 01). The government reserves the right to decide which performers, if any, are selected for the award. When a Stage 1 proposal is selected for potential award, the proposer will be notified by the government and will be required to submit a Stage 2 price/cost proposal for further consideration.

S. QUESTIONS & ANSWERS (Q&AS)

1. All questions regarding this notice must be submitted through the following link:

   ARPA-H Solutions
   ATTN: ARPA-H-MAI-24-01-05

   E-mails sent directly to the Program Manager, or any other addressee will be **discarded**.

2. All questions must be in English. ARPA-H will attempt to answer questions in a timely manner; however, questions submitted after the Q&A due date listed herein may not be answered.

3. In concert with this Announcement, ARPA-H will post Q&As regarding the Module Announcement on the ARPA-H UPGRADE webpage on a continual basis. ARPA-H encourages all proposers to review the Q&As provided before

submitting additional questions through the link in paragraph 1 of this Section. The government may not answer repetitive questions already answered in the posted Q&As.

T. PROPOSERS' DAY

The UPGRADE Program virtual Proposers' Day was held June 20, 2024. Details regarding the UPGRADE Proposers' Day are posted on the UPGRADE webpage. Attendance at the UPGRADE Proposers' Day is NOT required to propose to this module announcement.

APPENDIX A: SOLUTION SUMMARY TEMPLATE (SEE ATTACHED DOCUMENT)

ATTACHMENT 1: OTHER TRANSACTION BUNDLE (VOLUME 1) (SEE ATTACHED DOCUMENTS)

ENDNOTES

[1] https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983
[2] https://www.cnn.com/2024/02/28/tech/cyberattack-health-insurance-doctors-therapists/index.html
[3] https://www.fiercehealthcare.com/payers/optums-change-healthcare-responding-cybersecurity-issue
[4] 405d-hospital-resiliency-analysis.pdf (hhs.gov)
[5] Why hospitals, health systems are facing a cybersecurity talent shortage (beckershospitalreview.com)
[6] https://www.statista.com/statistics/1363111/average-duration-to-patch-vulnerability-by-industry/
[7] 2020_himss_cybersecurity_survey_final.pdf
[8] 50% of hospitals have been victims of a cyber-attack | Cyber Magazine
[9] Ransomware attacks on healthcare facilities cost $77.5B in downtime, report finds | Healthcare Dive
[10] https://www.globenewswire.com/en/news-release/2022/03/31/2413675/0/en/Largest-Healthcare-Data-Breaches-Reported-in-February-2022-Confirms-Need-for-Network-Security-Based-on-Zero-Trust-Microsegmentation.html
[11] https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983
[12] The Hospital Cyber Resiliency Initiative Landscape Analysis (HSCC)
[13] https://ieeexplore.ieee.org/abstract/document/10083125
[14] https://www.definitivehc.com/resources/healthcare-insights/us-hospitals-most-beds
[15] Zero Days, Thousands of Nights
[16] Health-ISAC. State of cybersecurity for medical devices and healthcare systems (2023)
[17] Philips Responsible Disclosure Statement | Philips
[18] Kaspersky finds 73% of healthcare providers use medical equipment with a legacy OS | Kaspersky
[19] https://www.statista.com/statistics/1363111/average-duration-to-patch-vulnerability-by-industry/
[20] https://hphcyber.hhs.gov/performance-goals.html
[21] ISO/IEC 7498 https://www.iso.org/standard/20269.html
[22] https://www.healthit.gov/sites/default/files/page/2022-07/Standards_And_Implementation_Specifications_Adopted_Under_Section_3004.pdf
[23] Examples of such open, consensus based standards include but are not limited to, the Digital Imaging and Communications in Medicine (DICOM) standard for medical image storage, the Global Alliance for Genomics and Health standards for storage of genomic data such as the Variant Call Format (VCF).