FEB 2021

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

2021-2025 STRATEGIC TECHNOLOGY ROADMAP OVERVIEW

Message FROM THE Chief Technology Officer

CISA Colleagues and Partners,

CISA continues to build on the opportunities to stand up a straightforward, repeatable, and transparent technology investment strategy. Our annual Strategic Technology Roadmap (STR) provides evidence-based recommendations to help you enable and influence future capabilities. I'm hopeful this Overview publication is useful and shows you where we are headed with STR Version 3 (STRv3). Over the next few pages, we'll discuss technology capabilities in development, desired future capabilities, and provide a forecast of the technologies CISA will look to invest in beyond 2025. The STR focuses exclusively on future technology capabilities to address persistent risks imposed by available technologies and future risks discovered from meta-analyses of hundreds of authoritative artifacts, and it is scoped for that purpose.

CISA's mission is to lead the national effort in understanding and managing cyber and physical risk. Guiding CISA technology investment towards the right mix of technology capabilities to best serve this mission is an evolving challenge. The STR serves as an annual touchstone for this challenge by identifying the technologies receiving current investments and revealing the opportunity areas for future growth.

On an annual basis, the STR examines how CISA defends today and secures tomorrow. To understand how we defend today, the STR:

1. Provides well-researched, evidence-based input to critical decision points that affect future CISA technology capabilities;
2. Identifies capability demands based on rigorous assessment criteria and provides recommendations regarding further use and development of technologies to meet the demands;
3. Applies methods to analyze selected, significant emerging standards to estimate potential risks;
4. Describes where capability demands identified in the previous STR are carried forward, where applicable, into this version;
5. Forecasts relevant capabilities based on formal research and development (R&D) pipelines; and
6. Speculates over the horizon technologies that could address specific cyber challenges.

STRv3 reveals to CISA and our partners the technology demand areas where increased investment through 2025 would have the greatest net effect. It does this by comparing current and near-term CISA technology investment with meta-analyses of research produced by CISA and our government and industry partners. STRv3 incorporates improved research and analysis methods to provide more accurate linkages and supportive rationale, from findings to recommendations, to form a guide for CISA technology investments.

STRv3 identifies 20 demand areas, organized into three technology domains – Cybersecurity, Communications, and Critical Enablers. We identify actionable recommendations for each demand area.

Looking to the future—the "securing tomorrow" element of our mission—we wrap up STRv3 with our projections of the capabilities CISA may have equities in developing beyond the 2025 horizon. Though some of these capabilities may currently exist in limited or isolated instances, they have the potential for wide adoption. CISA needs to be ready to embrace their development and capture their value as the technology reaches maturity. We welcome collaboration efforts from our colleagues and partners on these exciting future possibilities.

Brian Gattoni

CISA Chief Technology Officer

TABLE OF CONTENTS

INTRODUCTION

This overview summarizes the purpose and conclusion of the larger, more detailed CISA STR publication—a publication that is critical to informing senior leaders and harmonizing the CISA technology investment within the 2021 to 2025 timeframe. This document does not describe any particular CISA project and should not be seen as any kind of request for proposals or applications.

The STR—created in alignment with key CISA strategic planning documents—guides CISA technology investment towards achieving the agency's tailored capability goals of aligning and integrating our technology; maximizing our effect on cyber and critical infrastructure risks; and providing emergency communications. This overview provides high-level summaries of the STR's four sections:

CAPABILITY DEMANDS

Identifies capability demands based on artifacts such as security and vulnerability assessments. CISA identified these capability demands via analysis of hundreds of authoritative artifacts produced by CISA; federal, state, local, tribal, and territorial (FSLTT) partners; academia; and private industry. It categorizes the capability demands into 20 demand areas, organized into three technology domains, with actionable recommendations. The actions are standardized so that analysis will have consistent meaning in future STR reports. The standardized terms used across all capability demands are: ADOPT, DEMO (Demonstrate), INVEST, WATCH, DEFER, and DECIDE (decision to continue or stop).

TECHNOLOGY STANDARDS

Analyzes technology standards of significant interest addressing cybersecurity, critical infrastructure, and emergency communications. Based on criteria, the STRv3 identified standards requiring heightened situational awareness and participation to mitigate risk potential. As a new focus area for STR, we expect the analysis method to greatly improve and the findings to increase in value and outcome.

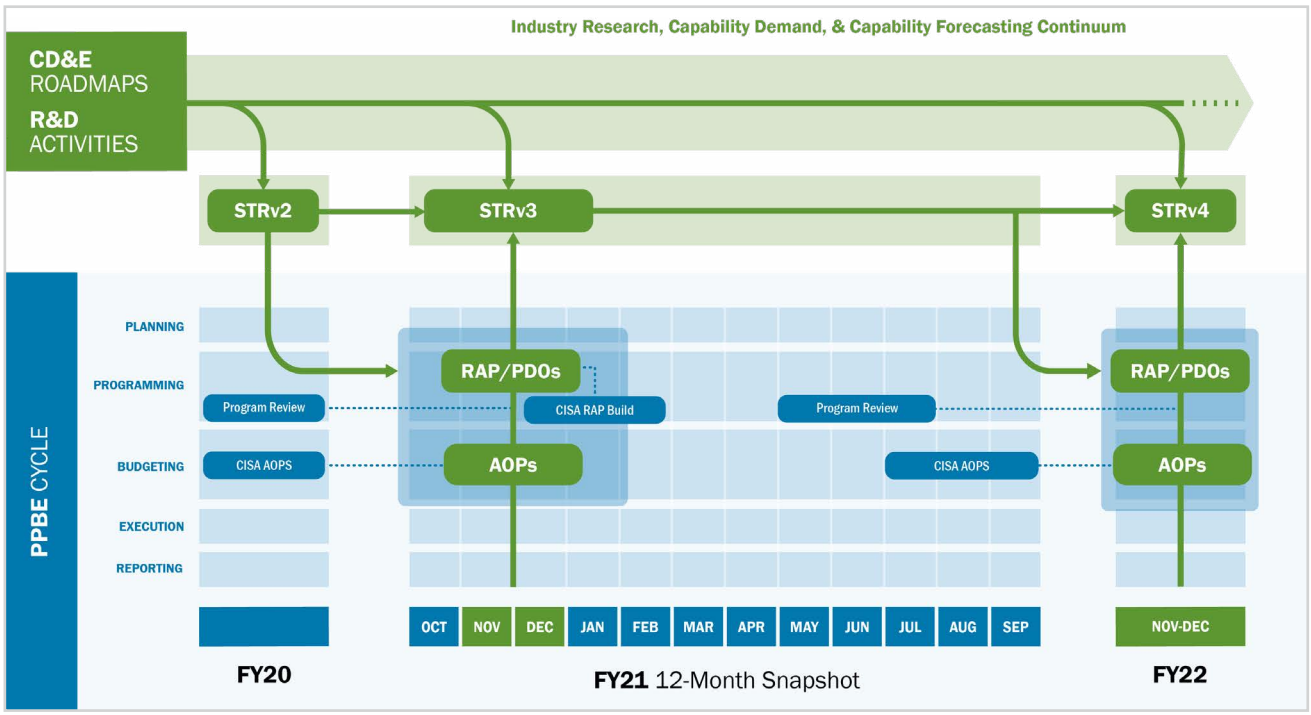
CAPABILITY FORECASTS

Aligns the capability demands to active R&D projects. For STRv3, CISA identified 23 relevant projects from DHS S&T, CISA NRMC, and DARPA based on specific criteria. These projects intersect with all but 5 of the 20 capability demand areas. These five gaps between capability demands and R&D projects represent opportunities to address risks through engagements and consultations, and to advance the state of the art through R&D.

TECHNOLOGY SPECULATION

Looks beyond the 5-year planning cycle at new and emerging technologies, technologies with potential for capturing significant market share or creating new markets, and technologies that present exceptional risks. In STRv3, this section focuses on two broad technology areas, each composed of many independently evolving technologies: Cross-Platform Information Exchange Management using blockchain technology; and Detecting and Countering Deepfake Technology.

TIMELINE AND INVESTMENT LOOP



The STR follows an annual publication cycle with delivery planned for early December each year and kick-off for the next version while the current version is in review. Throughout the year, the CISA Chief Technology Officer (CTO) team builds the STR by analyzing and integrating hundreds of artifacts such as CISA security and vulnerability assessments and gaps/requirements for portfolios of current CISA acquisition programs. The team also seeks to discover new, peer-reviewed studies that help to improve STR methods, analysis and findings, and recommendations.

To maximize STR utility, it aligns with CISA's planning, programming, and budgeting execution (PPBE) cycle, providing input to CISA strategic planning activities such as:

- program decision options (PDOs);
- the resource allocation plan (RAP), which details CISA's program funding;
- annual operating plans (AOPs) of each CISA division; and
- proposals for R&D submissions and lab projects

The output from strategic planning documents— as well as budget allocation from the PPBE process—feed into program plans, which provide input into future releases of the STR. This multi-faceted planning cycle increases the effectiveness of the technology investments necessary to fulfill the CISA mission.

CAPABILITY DEMANDS

Through analyzing hundreds of artifacts — from CISA, FSLTT, partners, and private industry—as well as ongoing research, CISA identified new capability demands since publishing STRv2 and verified capability demands to move forward from STRv2. Importantly, these combined capability demands are opportunities to build upon planned capability deployments and enhancements (CD&Es) with new technologies and to enhance the existing CISA Mission Environment (CME).

STRv3 categorizes the capability demands into 20 demand areas, organized into three technology domains derived from similarities among the capability demand areas. The 20 demand areas, organized into three technology domains: Cybersecurity, Communications, and Critical Enablers.

CYBERSECURITY

- Deception Technologies
- ICS Patching
- ML and Large-Scale Analytics
- ML and SOAR
- Network Systems Security
- Non-IP Based SCADA/ICS Protocol Monitoring
- Software Assurance and Vulnerability Management
- Vehicle Security
- Zero Trust Architecture (ZTA)

COMMUNICATIONS

- Cellular Security
- Computer-Aided Dispatch Interoperability
- LMR to Cellular Interoperability
- Mission Critical Voice on Cellular Network
- Next Generation Network Priority Services

CRITICAL ENABLERS

- Authoritative Time Source
- Digital Twin
- Distributed Enterprise Data Management
- EMP and GMD Disturbance Mitigations
- Risk Architecture and Advanced Analytics
- Single, Cross-Program Release and Change Management Tool

DOMAIN	DEMAND SCORES				
	< = 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	>5 YRS
CYBERSECURITY					
Deception Technologies	ADOPT				
ICS Patching	INVEST	DECIDE			
ML and Large-Scale Analytics	INVEST	DECIDE			
ML and SOAR	DEMO	DECIDE			
Network Systems Security	DEMO	DECIDE			
Non-IP Based SCADA/ICS Protocol Monitoring	INVEST/DEMO	DECIDE			
Software Assurance and Vulnerability Management	DEMO	DECIDE			
Vehicle Security	INVEST	DECIDE			
Zero-Trust Architecture (ZTA)	INVEST	DECIDE			
COMMUNICATIONS					
Cellular Security	INVEST	DEMO	DECIDE		
Computer-Aided Dispatch Interoperability	INVEST	DEMO	DECIDE		
LMR to Cellular Interoperability	INVEST	DECIDE			
Mission Critical Voice on Cellular Network	INVEST	DECIDE			
Next Generation Network Priority Services	INVEST	DEMO	DECIDE		
CRITICAL ENABLERS					
Authoritative Time Source	WATCH	WATCH	DEMO	DECIDE	
Digital Twin	INVEST	DEMO	DECIDE		
Distributed Enterprise Data Management	DEMO	DECIDE			
EMP and GMD Disturbance Mitigations	ADOPT				
Risk Architecture and Advanced Analytics	ADOPT				
Single, Cross-Program Release and Change Management Tool	ADOPT				

CAPABILITY FORECASTS

Commercial industry offers a wide range of products to address capability demands; however, there are conditions where product evolution may stop or slow (e.g., encounters a development plateau), or may not be commercially viable (e.g., a low demand/high development cost). Where commercial industry has no known or available solution due to these conditions, the STR defines linkages between capability demands and active R&D projects. CISA is partnered with DHS S&T for R&D projects to continuously track, forecast, and adjust its understanding of future capability demands and discover disruptive technologies that advance the state of the art and counter current, emerging, and potential adversary capabilities and other threats to the critical infrastructure.

STR identifies 12 DHS S&T R&D projects, 10 DARPA R&D projects, and 1 CISA NRMC project that support the 15 of the 20 capability demand areas.

It should be noted that Single, Cross-Program Change Management Tool is a commodity technology, so it would not be expected to have associated R&D projects—the exception to this understanding may be the increasingly complex nature of the .gov infrastructure as it migrates on and off premise into physical, virtual, and code-only instances of devices.

The ZTA concept is sufficiently mature for demonstrations, so it would also not be expected to have associated R&D projects. These gaps between capability demands and active R&D projects represent opportunities to further explore the state of the art and expected value in initiating new R&D projects.

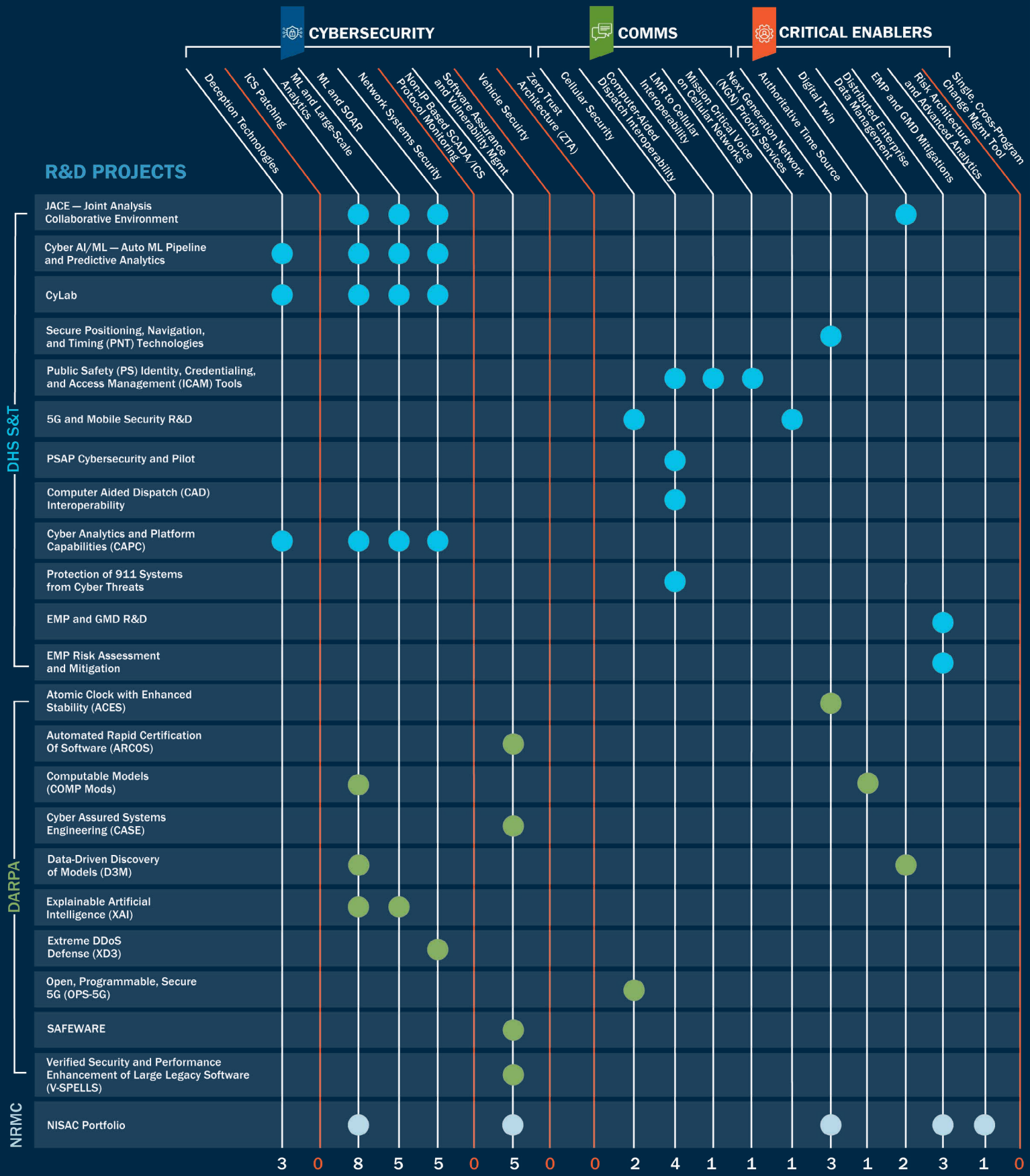
Mitigation actions to address these gaps include the definition of new requirements for R&D projects and a review of existing engagements and consultations, particularly where a demand is outside of CISA's direct influence or control.

The Joint Collaborative Environment (JCE), as recommended by the Cyberspace Solarium Commission, is a recent priority within CISA to address operational concerns. Many of the identified capability demand areas support implementing this new operational capability (e.g., Distributed Enterprise Data Management, ML – Large Scale Analytics, ML- SOAR, and Single, Cross-Program Release and Change Management Tool).

Implementing the JCE will necessitate coordinated development and implementation of new and existing capabilities across CISA. Data management and analytics are important technology underpinnings for the JCE upon which expected JCE outputs depend.

PROJECTS MAPPED TO CAPABILITY DEMAND AREAS

The following alignment of Capability Forecasts to the Capability Demand Areas illustrates opportunities for future R&D investments.



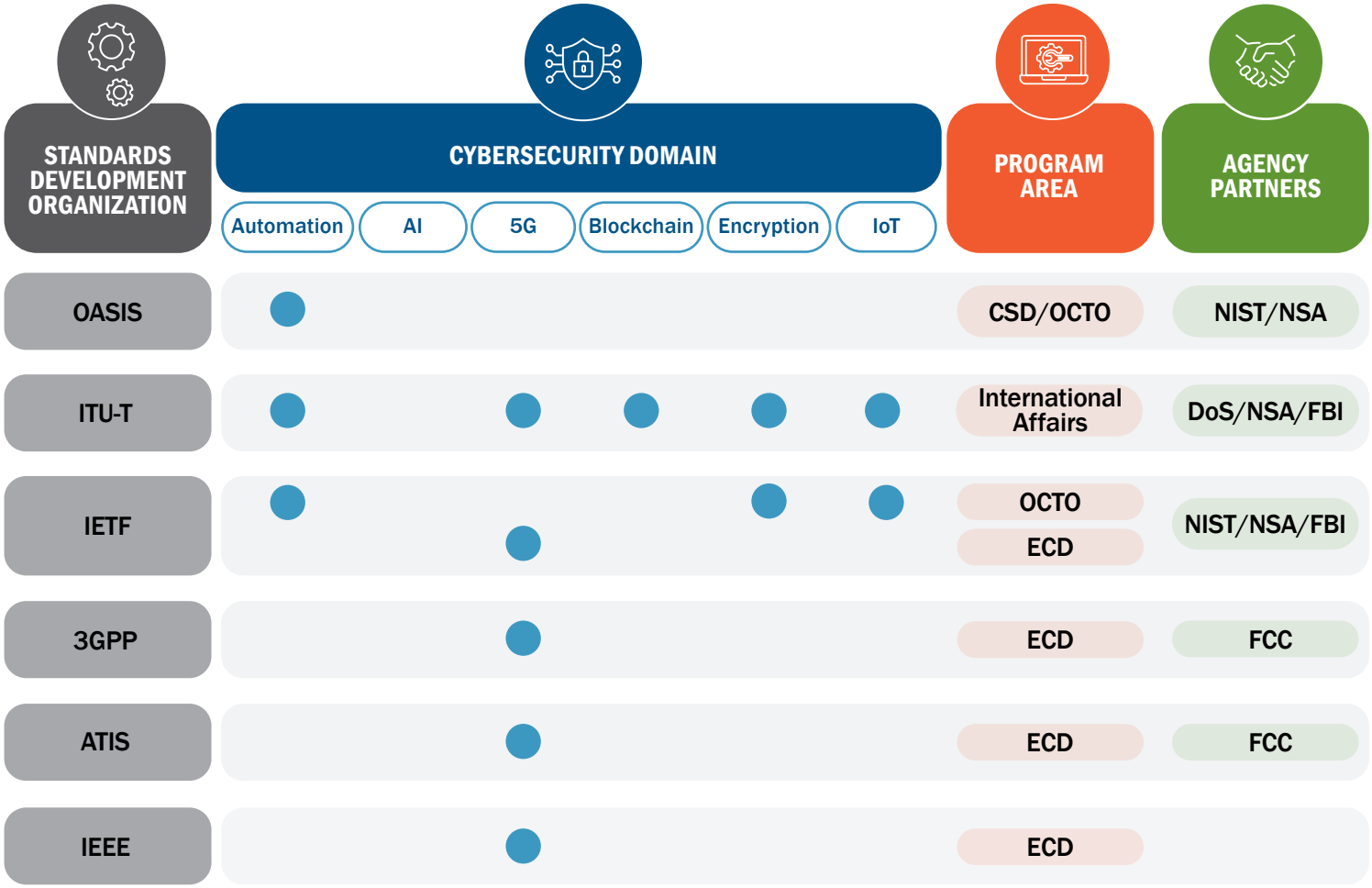
TECHNOLOGY STANDARDS

New in STRv3 is a method and analysis of technology standards with risk potential within the scope of the CISA mission. STR expands the view into future technologies by analyzing proposed technology standards that could be disruptive to cybersecurity, critical infrastructure, or emergency communications. CISA participation is encouraged with other government agencies to help monitor and influence emerging technology standards, and to maintain situational awareness and mitigate potential risks.

The table below provides qualitative assessments of various technology standards subjects against risk criteria derived from CISA's strategic priorities. Standards with multiple high ratings merit additional analysis to understand and mitigate potential risks.

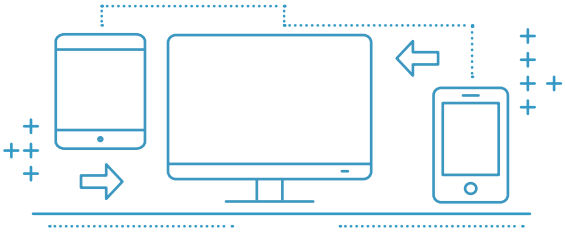
	STANDARDS SUBJECT AREAS				
RISK CRITERIA	5G	New IP	AI	PNT	Cloud
Potential to affect entities who perform National Critical Functions (NCFs)	HIGH	LOW	HIGH	HIGH	HIGH
Potential to empower, increase capability, and/or otherwise increase effectiveness of rivals and malicious actors	MEDIUM	HIGH	HIGH	HIGH	HIGH
Potential to reduce U.S. influence and participation in standards bodies; removes and/or shifts influence and participation to entities whose intent could result in negative consequences to U.S. interests	HIGH	HIGH	MEDIUM	LOW	HIGH
Results in new hardware, interfaces, or protocols that could disrupt CISA's mission to manage cyber and physical risk to the critical infrastructure	HIGH	LOW	HIGH	LOW	LOW
Introduces new methods of communication or significantly changes existing methods, reducing the effectiveness of CISA to protect and defend	HIGH	LOW	MEDIUM	LOW	HIGH
Introduces new security mechanisms that reduce the effectiveness, prevent or otherwise disable modern security capabilities	HIGH	HIGH	HIGH	HIGH	HIGH
Significantly alters architecture (compute, communications, storage, etc.) in which no security capabilities or reference architectures exist to protect U.S. interests	LOW	MEDIUM	MEDIUM	LOW	LOW

CISA, together with agency partners, currently participates in multiple standards organizations, across a range of technical subject areas.



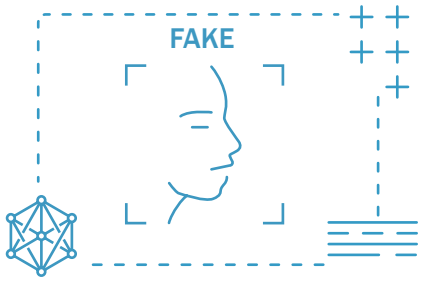
Looking beyond a five-year planning cycle, Technology Speculation looks at new and emerging technologies, technologies with potential for capturing significant market share or creating new markets, and technologies that present exceptional risks. The Technology Speculation section focuses on two broad technology areas, each composed of many independently evolving technologies: Cross-Platform Information Exchange Management using blockchain technology; and Detecting and Countering Deepfake Technology.

TECHNOLOGY SPECULATION



CROSS-PLATFORM INFORMATION EXCHANGE MANAGEMENT

Information exchange is fundamental to CISA's mission. However, much of CISA's information exchanges occur with decentralized policy enforcement for managing transactional records. This creates several challenges, one of which is the cross-platform management of information exchanges through centralized policy enforcement and transactional records tracking. A blockchain platform, a shared and secured data structure that maintains a transactional ledger that is immutable, could address this challenge. This approach would significantly enhance current means of information exchange traceability; data lineage tracking and provenance; smart contracts for access and sharing policies; and immutable/tamper-resistant records.



DETECTING AND COUNTERING DEEPFAKE TECHNOLOGY

Deepfakes are sophisticated computer-generated video or audio that is indistinguishable from reality. It was a concern during the 2020 election cycle and represents an outsized threat to CISA stakeholders and mission. As deepfake technology improves, automated detection and flagging of deepfake media will become more important. CISA is interested in monitoring the evolution of deepfake capabilities and anticipates future developments to protect against the use of deepfakes and mitigate occurrences. Today's deepfake capabilities are identified and mitigated through approaches which are reliant on the inherent limitations in deepfake production techniques. These limitations include absences of certain facial features such as glasses and beards, abnormal or non-existent eye blinking, inconsistencies in lighting and shadow, and simple facial overlays. A combination of these limitations and the availability of detection capabilities will likely minimize near term impacts of deepfakes. Future deepfake capabilities are not as well understood and expected to be virtually impossible to recognize and counter.

CONCLUSION
STRv3

CISA has developed the STR iteratively during the past three publication cycles—incorporating lessons learned, improving methods, and expanding coverage of mission relevant content—and will continue to do so with future versions.

In STRv3, CISA further refined methods and better aligned publication with the PPBE cycle. These improvements increased the STR's utility to the greater CISA community. STRv3 covers cybersecurity, critical infrastructure, and communications—the full spectrum of the CISA mission space.

The STR incorporates technology forecasts integrated from diverse sources. An annual review of the forecasted technologies will enable CISA to maintain the situational awareness of future technologies needed to identify trends that may affect stakeholder and government use cases, as well as the continually emerging technology changes that influence CISA's technology roadmap.

This annual technology forecasting will reduce the risks for potential technology investment deficits within the CISA mission space.

Looking further ahead to STRv4, in addition to tracking and forecasting capability demands, analyzing new and emerging technology standards, and speculating on the impact of over the horizon technologies, new dimensions will be added to enhance and broaden our understanding of future technologies.

We are developing methods to explore dimensions representing the economics of certain technologies, as well as technology risk probabilities in relation to strategic priorities.

ACRONYMS

3GPP	3rd Generation Partnership Program
5G	5th Generation
ACES	Atomic Clock with Enhanced Stability
AI	Artificial Intelligence
AOP	Annual Operating Plan
ARCOS	Automated Rapid Certification of Software
ATIS	Alliance for Telecommunications Industry Solutions
CAD	Computer Aided Dispatch
CAPC	Cyber Analytics and Platform Capabilities
CASE	Cyber Assured Systems Engineering
CD&E	Capability Deployments and Enhancements
CISA	Cybersecurity and Infrastructure Security Agency
CME	CISA Mission Environment
COMP Mods	Computable Models
CSD	Cybersecurity Division
CTO	Chief Technology Officer or Office of the CTO (OCTO)
CyLab	Cybersecurity Lab
D3M	Data-Drive Discovery of Models
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DHS S&T	Department of Homeland Security Science and Technology
DoS	Department of State
ECD	Emergency Communications Division
EMP	Electromagnetic Pulse
FBI	Federal Bureau of Investigation
FSLTT	Federal, State, Local, Tribal, and Territorial partners
GMD	Geomagnetic Disturbance
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
ITU-T	International Telecommunications Union – Telecommunications Sector
JACE	Joint Analysis Collaborative Environment
JCE	Joint Collaborative Environment
ML	Machine Learning
NCF	National Critical Function
NISAC	National Infrastructure Simulation and Analysis Center
NRMC	National Risk Management Center
NSA	National Security Agency
OASIS	Organization for the Advancement of Structured Information Standards
OPS-5G	Open, Programmable, Secure 5G
PDO	Program Decision Options
PNT	Positioning, Navigation, and Timing
PPBE	Planning, Programming, and Budgeting Execution
PSAP	Public Safety Answering Point
R&D	Research and Development
RAP	Resource Allocation Plan
SCADA	Supervisory Control and Data Acquisition
SOAR	Security Orchestration, Automated, and Response
STR	Strategic Technology Roadmap
V-SPELLS	Verified Security and Performance Enhancement of Large Legacy Software
XAI	Explainable AI
XD3	Extreme DDoS Defense
ZTA	Zero Trust Architecture

DEFINITIONS

ADOPT: CISA concludes industry and/or government should adopt or encourage adoption of a technology or capability.

DECIDE: An annual decision point has been reached to advance a program, project, technology, or capability to a next phase (e.g., from Demonstrate to Adopt), stay in the current phase, reset to an earlier phase, or cease further efforts.

DEFER: Significant uncertainty exists regarding the potential value and risk associated with these technologies. These items may represent leading edge research and experimentation. Government at large may have a role, such as proposed funding streams for quantum research; otherwise, no actions at this time.

DEMO: These items which have seen R&D investment are worth pursuing to understand how to build up the capability and incorporate it into the operations of a stakeholder or project that can tolerate the risk (e.g., pilot, prototype, large scale experiment). The Demonstrate phase is focused on ensuring that the value proposition can be maintained while the deployment risk is managed in order to justify operational integration.

INVEST: These items show significant value potential by improving operations or mission effectiveness and are currently or should be planned for investment (e.g., lab demonstration or experimentation, R&D Funding). The Invest phase is designed to "stabilize" an emerging technology, this may include experimentation, hiring of engineering, and developing a strategy for integrating an emerging technology into operational capabilities.

WATCH: These items are identified as worth exploring with the goal of understanding how it will affect CISA and stakeholder operations and/or improve mission effectiveness or reduce stakeholder risks, justifying further R&D or other investment in the future.


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY