FEB 2020

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

2020-2024 STRATEGIC TECHNOLOGY ROADMAP OVERVIEW

Message FROM THE Chief Technology Officer

CISA Colleagues and Partners,

As a relatively new agency, CISA has the opportunity to stand up a straightforward, repeatable, and transparent technology investment strategy. Our annual Strategic Technology Roadmap (STR) aims to do just that and I'm hopeful this Overview publication allows you to grasp where we are headed with STR Version 2 (STRv2). 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 investing in beyond 2025.

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 provides:

1. A detailed look of all capability deployments and enhancements (CD&Es) planned by CISA level 1 acquisition programs;
2. An integrated view across program roadmaps; and
3. Bridging terminology for the cross program CD&Es where nuances in program lexicon make it difficult to understand capability similarities and differences.

STRv2 reveals to CISA and our partners the technology demand areas not being met by our investment through 2024. It does this by comparing current and near term CISA technology investment with an analysis of technical security assessments produced by CISA and our government and industry partners. STRv2 identifies 14 new demand areas, 11 of which align to 27 candidate active R&D projects. The three unmet technology demand areas represent opportunities for collaboration with our colleagues and partners to fulfill those technology needs.

Looking to the future the "securing tomorrow" element of our mission we wrap up STRv2 with our projections of what capabilities CISA may have equities in developing beyond the 2025 horizon. Though some may sound like science fiction, the potential for their actualization is there and CISA needs to be ready to embrace their development. 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 lays out the purpose of the 100+ page CISA Strategic Technology Roadmap (STR) publication. Specifically, it identifies the priorities of STR version 2, 2020-2024 (STRv2) for organizations who are planning to develop candidate technologies to meet CISA capability demands. Additionally, it provides a high-level summary of STRv2—a publication that is critical to informing programs and harmonizing the CISA technology investment within the 2020 to 2024 timeframe.

The STR—created in alignment with key CISA strategic planning documents—guides CISA technology investment toward achieving the agency's tailored capability goals of aligning and integrating our technology. This overview provides high-level summaries of the STR's four sections:

CAPABILITY ROADMAPS

Presents an integrated view—across CISA level 1 acquisition program roadmaps—that surveys the 93 CISA capability deployments and enhancements (CD&Es)—either currently under development or planned for the next five years. It places the 93 CD&Es into 8 topic categories and maps them to the 5 NIST cybersecurity framework functions.

CAPABILITY FORECASTING

Aligns the newly identified capability demands to active R&D projects. For STRv2, CISA selected 27 candidate projects based on specific criteria. These candidate projects had intersects with all but 3 of the 14 capability demand areas. These three gaps between capability demands and R&D projects can inform organizations of new projects that may need to be created to address CISA equities.

CAPABILITY DEMANDS

Identifies new capability demands not already addressed by CD&Es in the Capability Roadmaps section. CISA identified these capability demands via analysis of 330 technical security assessments produced by CISA; federal, state, local, tribal, and territorial (FSLTT) partners; and private industry. It categorizes the new capability demands into 14 demand areas, which in turn map to 4 user domains and 5 capability categories.

BEYOND 2025: TECHNOLOGY SPECULATION

Looks beyond the 5-year planning cycle at the relationships between current market leading technologies, emerging technologies or those technologies with potential for capturing significant market share or creating new markets, and projects in the R&D pipeline. In STRv2, this section focuses on two broad technology areas, each of which are composed of many independently evolving technologies: Mesh of Things and production quantum computing.

AT A GLANCE:
CISA TECHNOLOGY INVESTMENT

As stated in the CISA Strategic Intent, **CISA's mission is to lead the national effort to understand and manage cyber and physical risk to our critical infrastructure**. To support CISA's "defend today, secure tomorrow" risk management mission, the CISA STR focuses on CISA investment in both current and future technology capabilities.

Specifically, it examines security and vulnerability assessments related to current capabilities to identify gaps, which along with an examination of emerging technologies help determine the demand for future capabilities (both near- and long term). It then aligns those capability demands with candidate technologies.

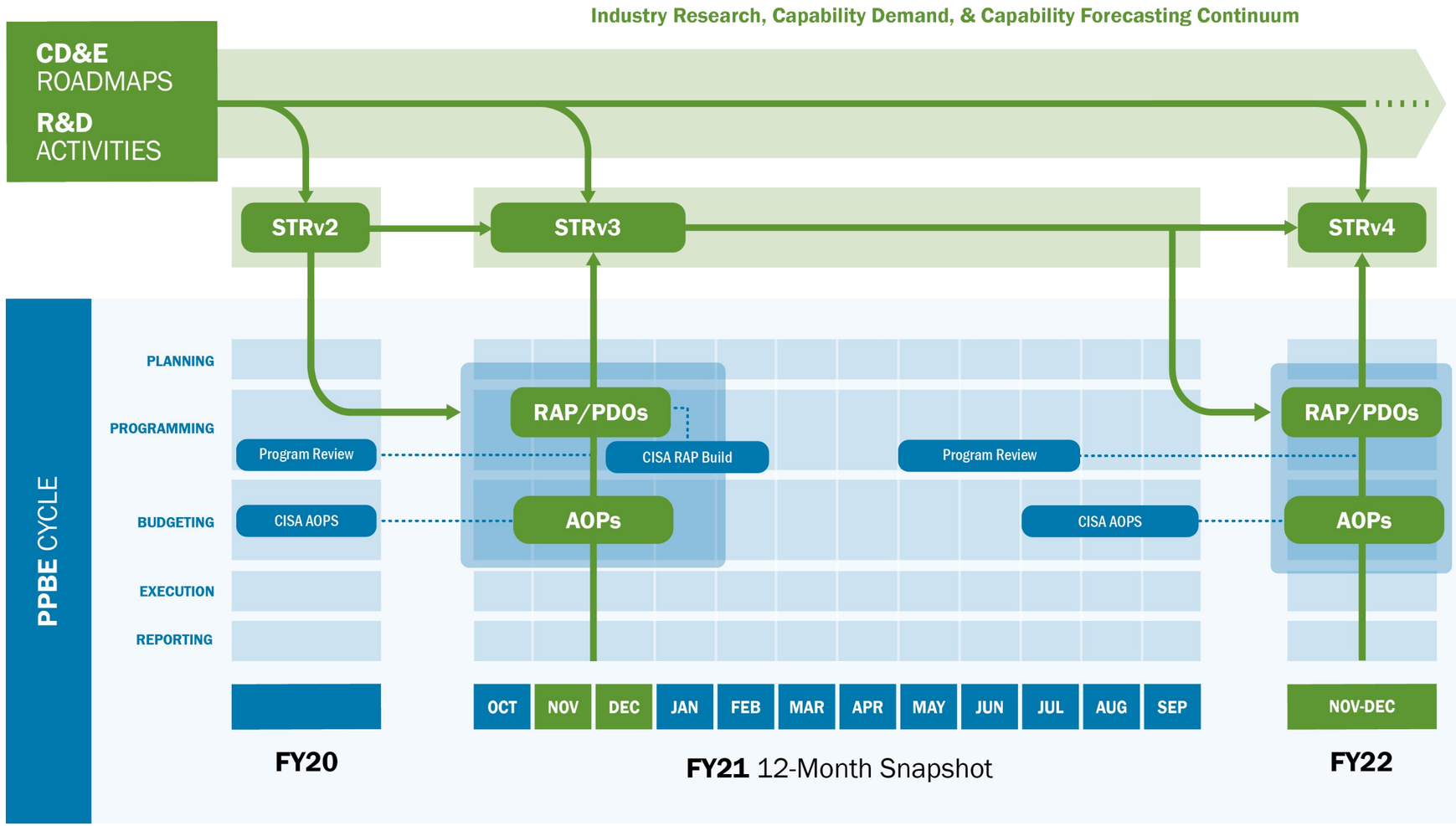
TIMELINE AND FEEDBACK LOOP

Beginning yearly in January, the STR follows an annual publication cycle with delivery planned for early December each year. Throughout the year, the CISA Chief Technology Officer (CTO) team builds the STR by analyzing and integrating CISA security and vulnerability assessments and roadmaps of current CISA acquisition programs.

The STR aligns with CISA's planning, programming, and budgeting execution (PPBE) cycle and the current STR serves as a foundational input to CISA strategic planning documents each year, including:

- program decision options (PDOs)
- the resource allocation plan (RAP), which details CISA's program funding
- the annual operating plans (AOPs) of each CISA division

In turn, 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 feedback loop supports a holistic planning cycle that aims to increase the effectiveness of the technologies necessary to fulfill the CISA mission.



STR & CISA
CAPABILITY ROADMAPS

One of the goals of the STR is to provide program managers with an integrated view across CISA acquisition programs and to impart a comprehensive understanding of CISA's investment in capability deployments and enhancements (CD&Es). This integrated view also serves as a means to inform technology researchers, systems developers, and decision makers on short to mid term program activities.

In general, the STR identifies CD&Es through surveying CISA acquisition programs and maps each CD&E to one of the eight STR capability categories:

- **INFORMATION SHARING**
- **NETWORK SECURITY & INFRASTRUCTURE MANAGEMENT**
- **ANALYTICS**
- **PREVENTION & DETECTION**
- **IDENTITY & ACCESS MANAGEMENT**
- **DATA PROTECTION MANAGEMENT**
- **ASSET DISCOVERY, CONFIGURATION, & PROTECTION MANAGEMENT**
- **DASHBOARDS**

STR ALIGNMENT WITH NIST

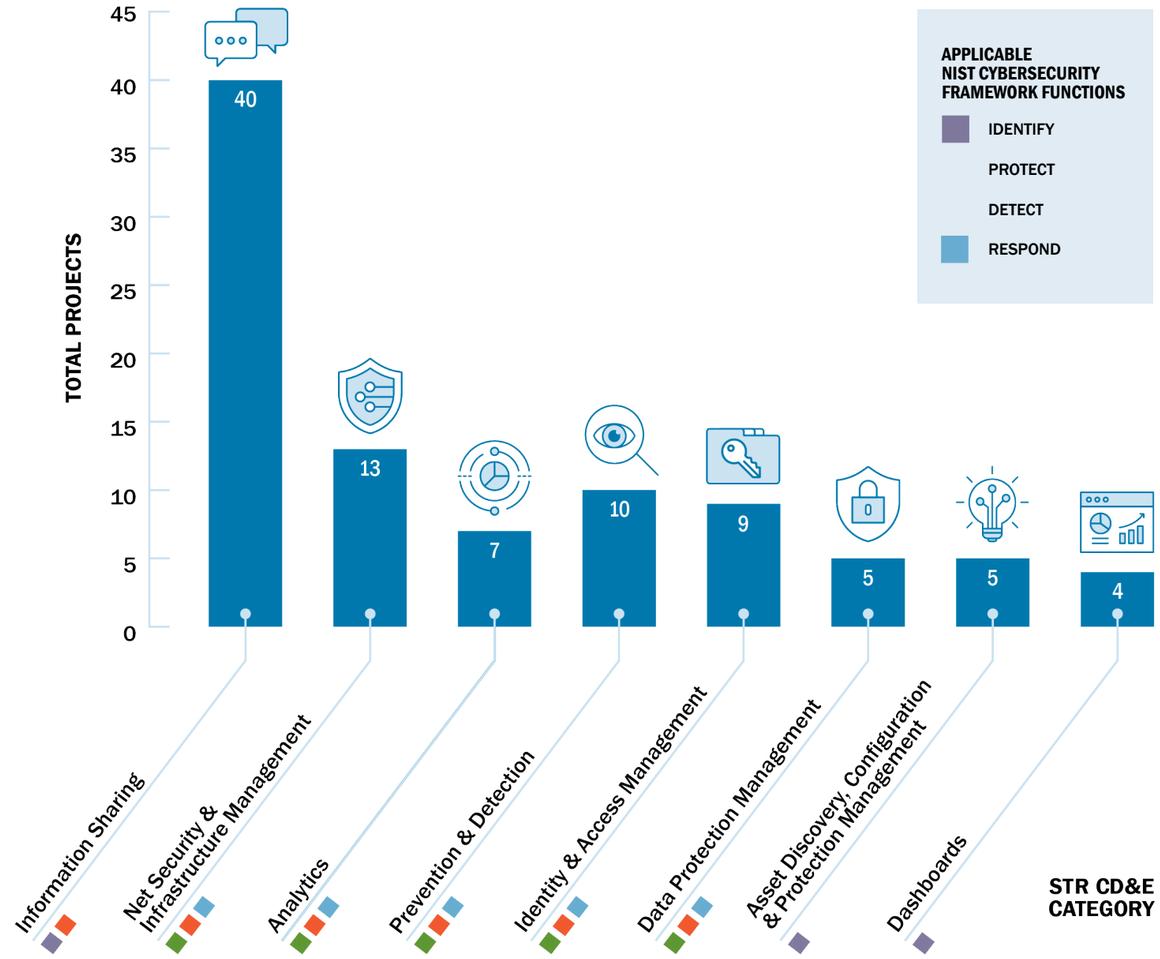
The STR also categorizes each CD&E currently in development—or planned for development within the next five years—under one or more of the five National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) functions:

- Identify
- Protect
- Detect
- Respond
- Recover[1]

[1]The STR only maps the capabilities in the program pipeline for deployment or enhancement; it does not map existing systems capabilities such as those that align to the NIST CSF Recover function.

STRv2
CAPABILITY DEPLOYMENTS & ENHANCEMENTS

STRv2 identified 93 CD&Es currently in development or planned for development within the next five years that mapped to the STR CD&E categories. Additionally, STRv2 categorizes the 93 CD&Es into one or more of the **Identify, Protect, Detect,** and **Respond** NIST CSF functions.[2]



[2]Although existing CD&Es may fall into the Recover function none of the STRv2 CD&Es currently in development—or planned for development within the next five years—maps to this NIST CSF function.

Through analyzing 330 technical security assessments from CISA, FSLTT, partners, and private industry as well as ongoing research, CISA was able to identify new capability demands. Importantly, these new capability demands are opportunities to build upon planned CD&Es with new technologies and to enhance the existing CISA Mission Environment (CME). These capability demands span the technology domains of Common Defensive Cyber Technologies, Common Defensive Cyber Operations Technologies, and Unique SLTT and Sector Partners Technologies.

STRv2 categorizes the new capability demands into 14 demand areas 7 derived from technical security assessments and 7 from ongoing research and development (R&D) efforts. The 14 demand areas, in turn, map to 4 user domains and 6 capability categories:

STRv2 CAPABILITY DEMANDS

1 COMMON DEFENSIVE CYBER TECHNOLOGIES (.GOV, SLTT, AND SECTOR PARTNERS)

1.1 PREVENTION AND DETECTION

1.1.1 Deception Technologies
1.1.2 Software Assurance and Vulnerability Mgt
1.1.3 Data Protection

1.2 ANALYTICS

1.2.1 ML – Large-Scale Analytics

2 COMMON DEFENSIVE CYBER OPS TECHNOLOGIES (.GOV, SLTT, AND SECTOR PARTNERS)

2.1 NETWORK SECURITY AND INFRASTRUCTURE MGT

2.1.1 ML – SOAR
2.1.2 Network Systems Security
2.1.3 Authoritative Time Source
2.1.4 Caller ID Spoofing
2.1.5 Mobile Device Security
2.1.6 Passwordless Authentication

3 UNIQUE SLTT & SECTOR PARTNERS TECHNOLOGIES

3.1 NETWORK SECURITY AND INFRASTRUCTURE MGT

3.1.1 Non-IP Based ICS/SCADA Protocol Monitoring
3.1.2 ICS Patching

4 COMMUNICATIONS

4.1 NATIONAL SECURITY/ EMERGENCY PREPAREDNESS (NS/EP) COMMUNICATIONS

4.1.1 Next Generation Network Priority Services (NGN-PS) for IP-Based Environment (Transition to IP-Based Communications)

4.2 EMERGENCY COMMUNICATIONS

4.1.1 CAD Interoperability

CISA Strategic Technology Roadmap Overview

STRv2 CAPABILITY FORECASTING

In STRv2, **CISA aligned 11 of the 14 STRv2 capability demand areas to relevant, active R&D projects**—both internal to DHS, in the DHS Science and Technology (S&T) directorate, and external. CISA used the following criteria to make selections:

The R&D project:

- has the potential to disrupt the basic functionality of private and public IT ecosystems;
- expands capabilities that may align with existing, planned, or future organizational functions;
- is not yet commercially available, meaning it is at some stage of formal R&D; and
- has the potential to counter known and unrealized/early pipeline adversary capabilities

Using this criteria, CISA was able to identify 27 candidate projects from DHS S&T and the Defense Advanced Research Projects Agency.

CISA was able to align candidate projects to all but 3 of the 14 capability demand areas:

1. Machine Learning (ML) and Security Orchestration, Automation, and Response (SOAR)
2. Next Generation Network Priority Services (NGN-PS) for IP-Based Environment
3. Computer-aided dispatch (CAD) Interoperability

CAPABILITY DEMAND AREAS GAPS

These three gaps between capability demands and R&D projects can inform organizations of new projects that may need to be created to address CISA equities.

1. ML AND SOAR

SOAR technologies enable organizations to automate IT security actions–such as log gathering, quarantining a file, hashing a file, or running an analytic. Organizations can then link these actions as well as non-security-specific actions together to execute security processes.

ML can augment SOAR capabilities by automating repetitive tasks. Incorporating ML into SOAR can also allow the automation of historical courses of action (COAs) taken by security analysts. Automating these can free up analysts' time that would otherwise be used determining the most appropriate COAs for given incidents.

The value of ML and SOAR to an organization is in these technologies enabling staff to focus on higher priority or strategic efforts.

2. NGN-PS FOR IP-BASED ENVIRONMENT

CISA collaborates with the public and private sectors to ensure the public safety and national security and emergency preparedness (NS/EP) communications community has access to priority telecommunications and restoration services to communicate under all circumstances. CISA is currently executing an NGN-PS acquisition program to evolve priority service capabilities from circuit-switched to IP-based packet-switched networks.

Note: as the roadmap for the CISA level 1 acquisition program, Next Generation Network Priority Services (NGN-PS) was unavailable during STRv2 development, the CISA CTO team analyzed NGN-PS artifacts to derive capability demands.[3]

NGN-PS will enable NS/EP users to have priority voice, data, and video communications as the communications networks evolve.[4] The effectiveness of NGN-PS has a direct effect on NS/EP users' ability to perform essential job functions. NGN-PS should benefit public safety communications by ensuring that first responder voice, video, and data capabilities are operational during a national emergency.

The evolving NGN-PS program must address priority data, video, and information services capabilities on the service providers' wireline and wireless IP telecommunications networks. Priority data services should include services such as email, SMS, streaming video, enterprise access, web access/browsing, and other currently used data services. Many of these data services use the public internet either completely or partially. The role of the network within the priority services platform is to enforce priority levels on traffic associated with priority users. There are several factors critical to this enforcement function:

- The priority user must be authenticated and authorized to receive priority treatment.
- The network must be able to uniquely identify priority user traffic and associate the authorized level of priority to that traffic.
- The network must have prioritization means to apply to the identified traffic.
- For cases where networks interconnect, traffic prioritization indicators must be securely passed to interconnected networks for downstream prioritization.

3. CAD INTEROPERABILITY

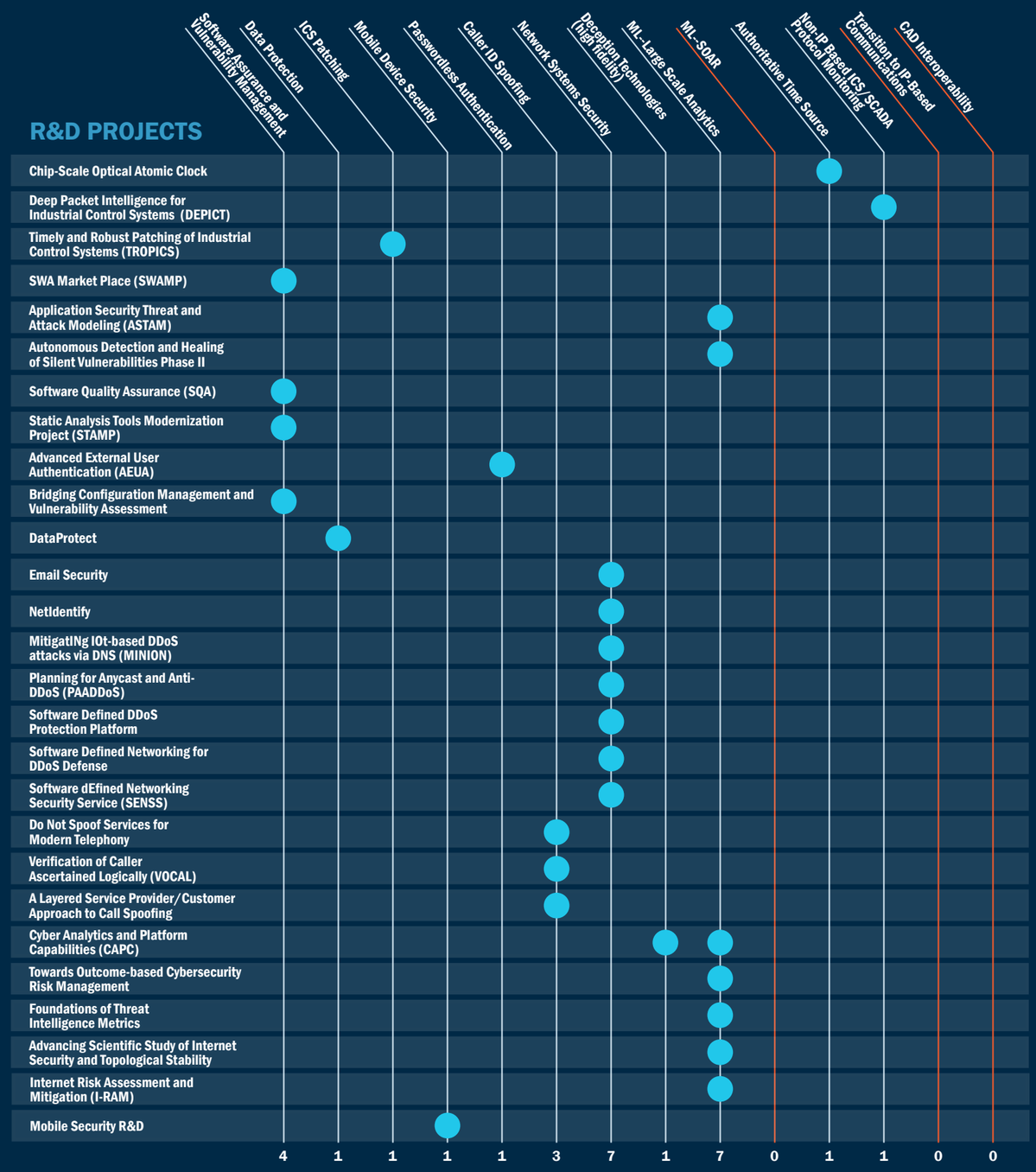
CAD-to-CAD interoperability enables emergency responders to share vital data and voice information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. Although it is often assumed that emergency response disciplines and jurisdictions already seamlessly coordinate with each other, the current reality is that jurisdictions across the United States have a ways to go before fully actualizing CAD-to-CAD interoperability for data and voice communications.

Because it automates the dispatch of resources based on proximity to the incident and type of resources required, CAD-to-CAD interoperability reduces response time, potentially saving lives. However, the realization of interoperability is threatened by other emerging technologies and a lack of standardization among solutions. CISA intends for its technology investment in interop erability to help develop a stan dardized information exchange, technical data exchange model and dictionary, and a standard reference architecture that includes necessary cybersecurity capabilities.

[3]STRv3 is targeting all technology-related acquisition programs.
[4]CISA. (2019, July 17). Emergency Communications Division Priority Telecommunications Services. Retrieved from https://www.cisa.gov/emergency-communications

R&D PROJECTS MAPPED TO CAPABILITY DEMAND AREAS

See table for the list of R&D projects that map to the 11 capability demand areas. STRv2 provides project descriptions. CISA encourages interested readers to contact CISA Chief Technology Office via the CISA Service Desk for further details concerning these R&D projects.



The final section of STRv2 looks past CISA's 5-year planning cycle to the relationships between:

- Current market leading technologies,
- Emerging technologies or those technologies with potential for capturing significant market share or creating new markets, and
- Projects in the R&D pipeline.

STRv2 focuses CISA technology speculation on two broad technology areas, each of which are composed of many independently evolving technologies: Mesh of Things and production quantum computing.

MESH OF THINGS: SELF-ORGANIZING INFRASTRUCTURE AND SERVICES DELIVERY

The growth of the Internet of Things (IOT) is continuing to pick up momentum, driving research and development focused on the "Mesh of Things," a code-based, self-healing infrastructure that may move computing workload and data storage to an increasingly decentralized architecture. Because this move pushes power and storage demand closer to the consumer, it may enable greater compute and storage capabilities for higher-order analytics. The end result will be faster networks and—due to characteristics of mesh device relationships and the mesh's self-healing infrastructure—significantly greater resilience. The latter result makes the Mesh of Things of particular interest to CISA.

PRODUCTION QUANTUM COMPUTING

Quantum computing allows for many states to concurrently operate classical analog algorithms in parallel rather than the serial approach of traditional computing. This speed can both enable more powerful means of encryption and concurrently make existing encryption capabilities ineffective. The source of this speed is quantum particles—qubits—that can exist in a simultaneous state of both 1 and 0. The beauty of qubits from a cyber-security perspective is that, if a malicious actor tries to observe them in transit, their super-fragile quantum state "collapses" to either 1 or 0, thus protecting the data. Because quantum computing has the potential, someday, to both positively and negatively impact the security of communications systems, CISA is interested in its ongoing research and development, particularly as commercial and academic communities drive toward quantum supremacy.

CONCLUSION
STRv3

CISA has developed the STR iteratively incorporating lessons learned, improving methods, and expanding coverage to the entire agency and will continue to do so with future versions.

STRv1, released in early 2019, focused exclusively on CISA's National Cybersecurity Protection System (NCPS) and the Continuous Diagnostics and Mitigation (CDM) programs. STRv1 relied primarily on the findings of CISA's .govCAR technology security assessments as the basis for identifying capability demands.

STRv2 added CISA's Next Generation Network Priority Services (NGN PS) programs, significantly improved analysis methods, and a wider swathe of security and vulnerability security assessments for identifying capability demands and forecasting capabilities. CISA applied STRv2 to its resource allocation plan (RAP) and program decision options (PDOs). STRv2 also delivered the basis of a new reference architecture. In addition, it delivered specific findings and recommendations as output from extensive analysis across hundreds of artifacts.

In STRv3, CISA expects to further refine methods and better align publication with the planning, programming, and budgeting execution (PPBE) cycle; doing so will improve the STR's utility to the greater CISA community. STRv3 will cover cyber, critical infrastructure, and communications the full spectrum of the CISA mission space.

STRv3 will also include new content on standards bodies and emerging standards of interest. Specifically STRv3 will focus on identifying standards in their early development that could impair CISA's ability to successfully execute mission or have some other negative effect on national security interests.

Looking further ahead to STRv4 while it's too early to speculate on content one objective will be to produce multiple versions for specific audiences. For example, CISA will develop a vendor/manufacturer version for industry day types of events, an online interactive version that allows viewers to isolate content through point and-click actions on live charts, and a formal publication for others—including decision-makers, the acquisition executive, program managers, and systems engineers—responsible for continuously evolving CISA's technology capabilities beyond those of the Nation's adversaries.


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY