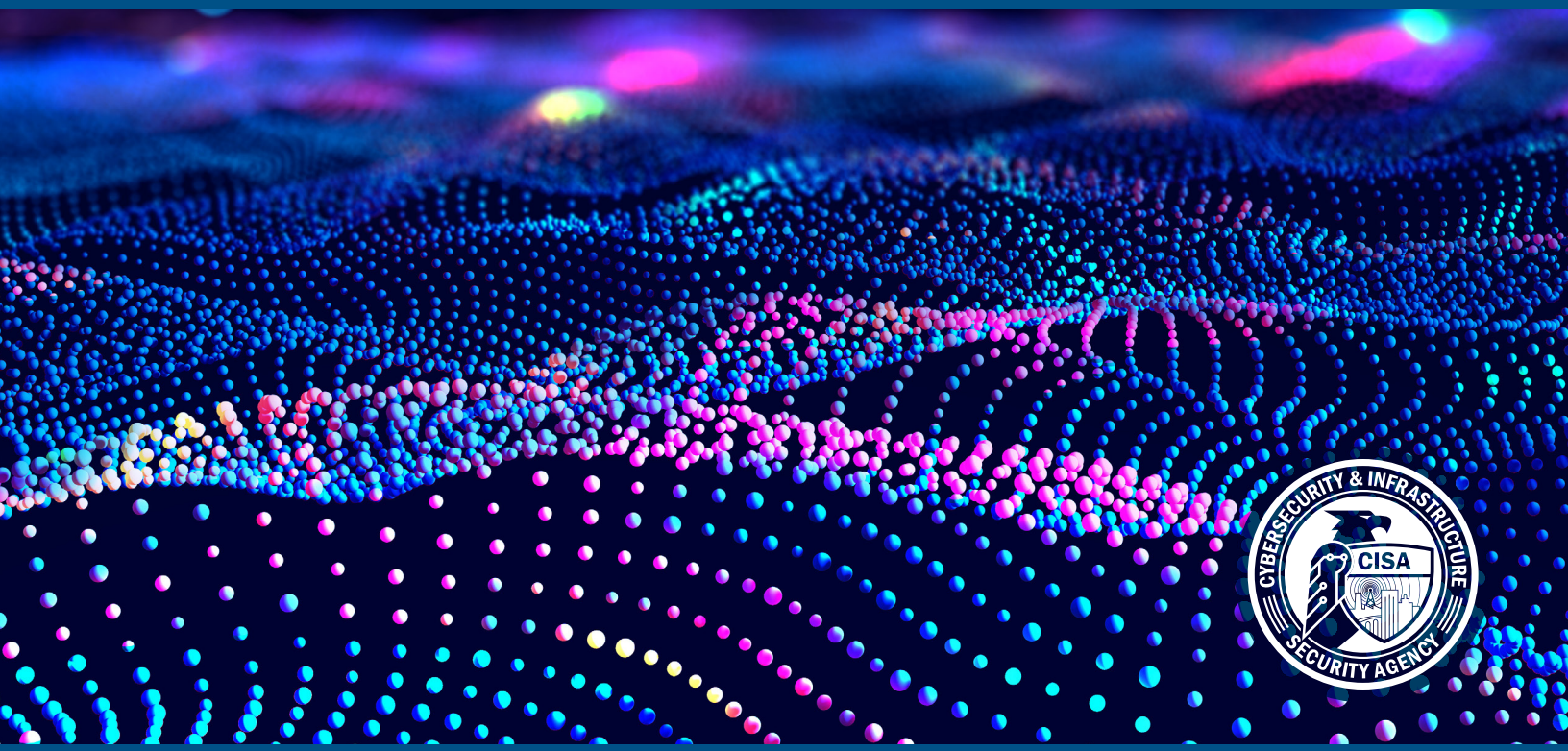
ONE CISA: COLLABORATION, INNOVATION, SERVICE, ACCOUNTABILITY

2023-2027

STRATEGIC TECHNOLOGY ROADMAP

VERSION 5



PUBLICATION: NOVEMBER 2022 | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

MESSAGE FROM THE CHIEF TECHOLOGY OFFICER

CISA Colleagues,

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 Summary publication is useful and shows you where we are headed with STR Version 5 (STRv5). Over the next few pages, we'll discuss technology capabilities in development, describe desired future capabilities, and provide a forecast of the technologies CISA may look to invest in beyond 2027. 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. The STR is scoped for these purposes.

CISA's mission is to lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. Guiding CISA technology investment toward the right mix of technology capabilities to 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. Describes where capability demands identified in the previous STR are carried forward, where applicable, into this version;
4. Forecasts relevant capabilities based on formal research and development (R&D) pipelines; aligning capability demands with capability forecasts; and
5. Speculates about "over the horizon" technologies that could address specific cyber challenges.

STRv5 reveals the technology demand areas where increased investment through 2027 would have the greatest net effect. It does this by comparing current and near-term CISA technology investment with meta-analysis of research produced by CISA and our government and industry partners. STRv5 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.

STRv5 identifies 15 capability demand areas, organized into three technology domains – Cybersecurity, Communications, and Critical Enablers. There are 43 technologies associated with the 15 capability demand areas in STRv5. We identify actionable recommendations for each demand area. STRv5 updated 20 technologies carried forward from STRv4 and added 23 new technologies.

Looking to the future—the "securing tomorrow" element of our mission—we wrap up STRv5 with our projections of the risks and capabilities beyond 2027 that CISA may further explore. Though some of the aspects of these capabilities may currently exist in limited or isolated instances, they have great potential for scalable effect when these capabilities mature. CISA needs to be ready to embrace development of these capabilities 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

Contents

INTRODUCTION

The CISA STR provides a roadmap to maintain and evolve technological superiority over our Nation's adversaries, to protect and defend against critical infrastructure (CI) threats, and to sustain resilient emergency communications. The STR is designed to guide CISA technology investments, through a foundation based on rigorous research and identification of best practices for industry and government cybersecurity and communications capabilities, to achieve the agency's mission needs. Systems that enable the operation of all levels of government and systems that control and operate the utilities on which we all depend (such as electricity and water) face significant cyber-based threats that are among the most substantial and growing threats to our Nation. Degradation, destruction, or malfunction of government and CI systems could cause serious human and economic harm, ultimately posing a threat to U.S. national security.

To address these threats and enable CISA's mission, the CISA OCTO develops the STR through a continuous cycle of technology analysis, risk prioritization, future capability definition, and strategy integration. With detailed findings and recommendations from a broad and deep, forward-looking view into the technologies that will enable CISA's mission; the STR guides CISA's technology investment and establishes a feedback loop between complex and competing technology priorities. The STR is reviewed and updated annually to account for technology trends, breakthroughs, and commercialization, as well as changing CISA priorities and capability demands that may impact previous recommendations. This process renews the STR each year, ensuring its responsiveness to the development and deployment of new CISA capabilities and to the evolution of adversary techniques, both known and not yet realized.

The STR supports and integrates with CISA strategic planning documents. It bridges tactical and strategic planning by providing a framework and context from which to make well-informed investment decisions that help ensure CISA is interoperable, efficient, and responsive to national security priorities. Continuous alignment between the STR and CISA strategy will ensure that capability demands and capability forecasting not only reflect findings reported in security and vulnerability assessments but will also define the capabilities and technologies necessary to evolve CISA and its support and services to Federal, State, Local, Tribal, and Territorial (FSLTT) governments, as well as CI owners and operators. The STR's capability demand and capability forecasting enhances decision-making, prioritization, budgeting, and programming; thereby offering a more predictable, integrated, and intentional technology acquisition process and timeframe.

The STR public release presents findings and recommendations in the form of slick sheets or single page summarizations of technologies categorized as capability demands, capability forecasts, and technology speculation. Each slick sheet is intended to address important questions such as: (1) what is the technology; (2) what did we find/what do we recommend; (3) why should CISA care; and (4) is it something CISA would operate or apply to consultations with FSLTT, private industry, and other partners. To present succinct, executive-level STR output, content such as citations, acronyms, and extended definitions were intentionally omitted, but are available in upon request and where releasable. Any reference to specific commercial products, processes, services by service mark, trademark, manufacturer, or otherwise is provided for informational purposes and does not constitute or imply endorsement, recommendation, or favoring by CISA.

ICS SECURITY
ASSET DETECTION FOR ICS

Asset detection in the operational technology (OT) environment is a foundational aspect of every critical infrastructure (CI) operator's cybersecurity program. Automated asset detection capability reduces the work required by industrial control system (ICS) cybersecurity defenders to gain a full asset inventory and configuration control of the OT environment. Unfortunately, a fully automated, vendor agnostic asset detection capability is not available in the ICS ecosystem.

Tools to support asset detection for ICS are provided by ICS device vendors and cybersecurity tool vendors. ICS device vendor tools typically support only the vendor's devices. At this time no single tool is available that can provide universal (all vendors) ICS asset inventory management (including discovery and configuration control). In addition, asset management should operate continuously to ensure changes are detected as close to real-time as possible. Candidate technologies include network attached monitoring and asset/chassis bus connected monitoring technologies.

The security risk factors created by a lack of full and continuous asset knowledge include malicious rogue devices, device failures, and asset configuration changes. Any of these or other conditions where asset information is incomplete can lead to the introduction or exploitation of asset and system vulnerabilities.

FINDINGS & RECOMMENDATIONS

CISA should adopt and encourage CI operators to adopt automated ICS asset discovery tools. CISA should encourage asset detection vendors to continue to expand the scope of ICS devices their tools support. The payback is a reduced risk probability factor of successful cyber-attacks on CI.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Asset Detection for ICS	Adopt				

ICS SECURITY

FAULT TOLERANT/RESILIENT CYBER PHYSICAL SYSTEM

Supervisory Control and Data Acquisition (SCADA) and industrial control system (ICS), systems control processes that combine, modify, and transfer inputs to create outputs by manipulating physical devices or objects. A few examples of controlled processes with large moving parts (e.g., turbines, motors) are energy generation, manufacturing, and ship control. In these and similar examples, the inertia of the devices or objects under control can protect the systems. Inertia is a physical property of matter defined as the resistance of a physical object to a change of its speed or direction when an external force acts on that object. ICS can utilize the inertia of the physical components within the process under control to detect and mitigate attacks on the process. An example is the inertia of a rotating steam turbine in an electricity generation plant. The inertia of the turbine can be exploited to protect the process under control (electricity generation) when coupled with security components that detect and mitigate anomalous ICS commands in near real time.

Navy NAVSEA has demonstrated a solution termed Resilient Hull, Mechanical, and Electrical Security (RHIMES) based on this principle. The candidate technology detects attacks at each process control point by monitoring the outputs from two or more parallel ICS controllers implemented with different, but functionally identical, software or firmware. The attack is mitigated by detecting inconsistencies in the outputs and then stopping controller operations, resetting the system, and resuming normal operations within the timing requirements of the process under control.

FINDINGS & RECOMMENDATIONS

CISA should support further demonstrations of this technology. The goal is to communicate to CI sectors that this technology is valuable. The benefit is a reduced risk of successful cyber-attacks on ICS.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Fault Tolerant ICS/RHIMES Technology	Demo				

ICS SECURITY

ICS PATCH AUTOMATION

Industrial control systems (ICS) often do not receive software patches in a timely manner. ICS owners and operators do not apply patches for many reasons, including the risk or cost of disruption of operational processes and the failure of vendors to provide patches for specific equipment. Regardless of the reasons, the failure to apply patches leaves ICS devices and systems vulnerable for much of the time they operate. Left unaddressed, the vulnerabilities can threaten production or safety and increase the attack surface of the operation. The potential impacts of not patching include physical destruction of equipment or facilities, economic losses, and personal safety incidents

Patch management technology and processes can reduce ICS vulnerabilities. Patch management processes include analyzing patches for criticality, time sensitivity, and testing requirements, which can improve patch deployment decisions and timelines. Additionally, automating patch deployment could assist in expediting the patching process. Automation can include unit and system testing, as well as patch deployment.

The security risk factors associated with unpatched ICS include remotely exploitable software vulnerabilities, consequences such as process control failures, reduced or blocked ICS process management, and creation of deceptive process status. Successful exploitation of a vulnerability leading to any of these (or other) threat events or consequences could cause significant physical, economic, and personal safety impacts.

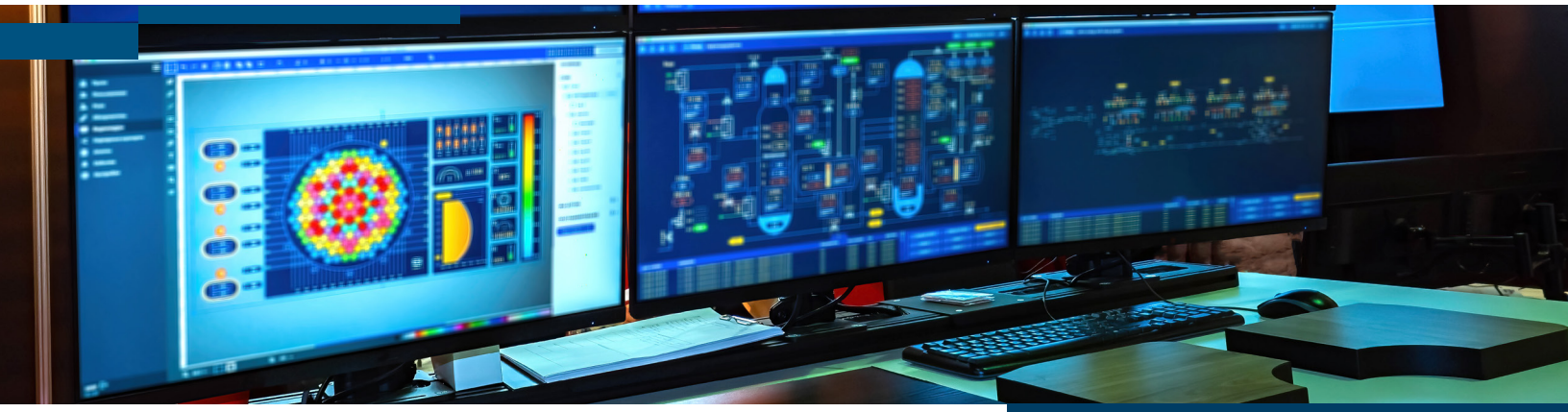
FINDINGS & RECOMMENDATIONS

Given the potential for cascading failures from attacks on ICS systems in the CI sectors, CISA should consider supporting R&D efforts to improve ICS Patch Automation. Organizations such as Electric Power Research Institute (EPRI) and Pacific Northwest National Laboratory (PNNL), among others, are working to improve the cybersecurity of ICS environments (networks and devices). CISA should also support efforts to encourage CI operators to adopt ICS patch management capabilities. These efforts can reduce the probability of successful cyber-attacks on private and Federal, State, Local, Tribal, and Territorial (FSLTT) operated CI.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
ICS Patch Automation	R&D				

ICS SECURITY

MACHINE LEARNING (ML) ENABLED SCADA IDS ANOMALY DETECTION



Machine Learning (ML) analytics are being applied to ICS/ Supervisory Control and Data Acquisition (SCADA) intrusion detection systems (IDS). ICS cybersecurity is positioned to use ML techniques due to increasing volumes of data, and a shortage of highly skilled analysts able to make sense of the myriad of data collected from sensors, systems, networks, cyber threat intelligence feeds, and process analytics. Two approaches to SCADA anomaly detection are currently being pursued in research and industry: data-centric and design-centric. The data-centric approach uses the SCADA network traffic, commands, and responses to learn the normal sequences and cadence for processes under control. The design-centric approach is based on a model of the process under control. The design-centric approach also uses real-time SCADA commands and responses to monitor the process and detect anomalous process deviations, commands, or responses.

The target gaps for this technology are the lack of highly skilled analysts, removal of human analysis errors, and the difficulties in hiring experienced personnel to support the 24/7 operations tempo of today's Security Operations Centers (SOCs). ML enabled SCADA IDS anomaly detection can partially address the target gaps by improving the detection capability and situational awareness development for SOC analysts. The security risk factors addressed by ML enabled SCADA IDS anomaly detection include system vulnerabilities, undetected anomalous SCADA commands and responses, and lack of situational awareness.

FINDINGS & RECOMMENDATIONS

CISA should adopt ML enabled SCADA IDS anomaly detection to serve ICS partners and encourage CI stakeholders to implement, as appropriate, into their operations centers. CISA may also recommend further study and monitoring of academic research of ML enhancements that improve the transparency/understandability of the ML decisions, recommendations, and false positive reduction techniques. The Control Environment Laboratory Resource (CELR) testbed may offer ICS cybersecurity research capabilities to support these study areas.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
ML Enabled SCADA IDS Anomaly Detection	Adopt				

ICS SECURITY

INTEGRATED PHYSICAL AND CYBER SIEM

The integration of physical sensor data with traditional Security Information and Event Management (SIEM) focuses on one of two related efforts: (1) integration of data sources from traditional physical security mechanisms, such as badging systems and video cameras, with inputs from traditional cyber-only SIEM tools; and (2) security of Cyber Physical Systems, which are "engineered systems that are built from, and depend upon, the seamless integration of computation and physical components." Such integration can identify abnormal situations that may evade detection by methods relying on information from either the physical or cyber domain alone.

The sources and formats associated with events are widely disparate and mostly proprietary. Physical data sources may include badge or key card systems, fire and security alarm systems, closed circuit television cameras, lighting, and climate controls along with their associated sensors and internal phone or intercom systems. The sources of audit and logging data are equally varied and are seen at all levels of the software stack, from network infrastructure components and system logs to application monitors. Multiple efforts to establish a common framework for SIEM data derived solely from cyber-sources have either failed to achieve widespread acceptance or are too narrowly focused (e.g., spam and malware). One project, Intrusion Detection Message Exchange Format (IDMEF) v2, declares itself to be "an international consortium promoting format standardization in cybersecurity." However, there are few references to it in technical literature, and the most recent versions were released more than 18 months ago.

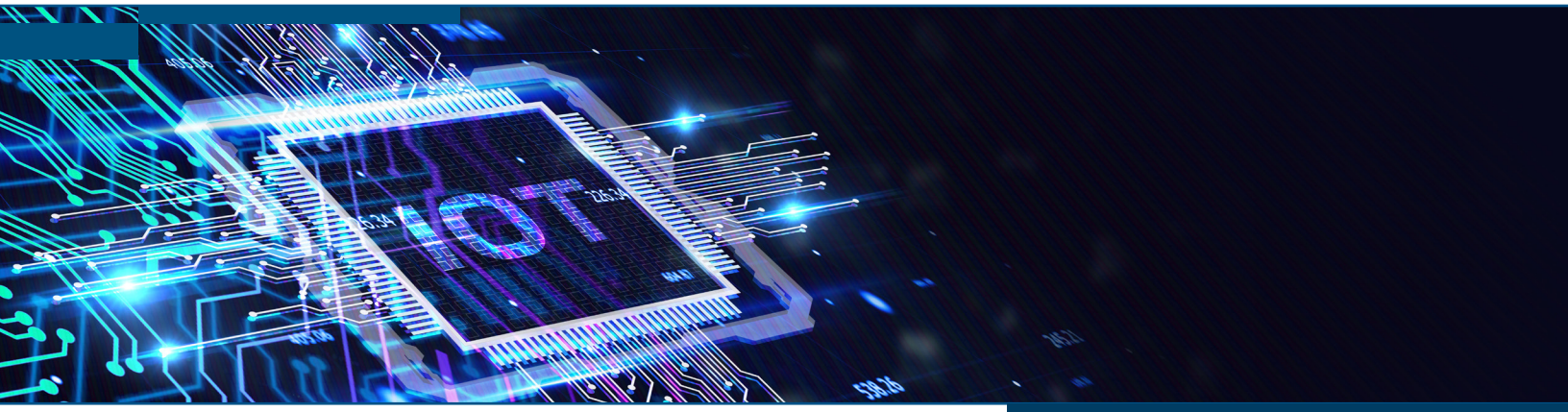
FINDINGS & RECOMMENDATIONS

CISA should initiate research that fully explores the current state of work in this area and identify impediments to its progress. Based on the results of that effort, CISA should formulate an approach that includes standards bodies and private sector incentives as appropriate.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Intergrated Physical and Cyber SIEM	R&D				

IoT SECURITY

IoT DEVICE SECURITY



Billions of small devices composed of embedded sensors and network connectivity, otherwise known as Internet of Things (IoT) devices, are being used in a diverse set of applications. More recently, the use of IoT devices has grown within the CISA mission space to perform critical remote sensing, industrial control, and physical security tasks. Unfortunately, IoT devices usually lack traditional end point security features and other cybersecurity controls. As a result, threat actors use IoT devices to eavesdrop, control devices or the systems to which they are attached, conduct large scale denial of service (DoS) attacks, or conduct cryptocurrency mining operations.

Because of the growing use and criticality of IoT devices and networks, both government and industry continue to develop better security controls for these devices. These technologies include on-board malware detection, secure on-boarding protocols, and lightweight cryptography (LWC). Secure on-boarding protocols help prevent attackers from compromising IoT devices; and on-board malware detection identifies a device controlled by an adversary. Lightweight cryptography can be used to secure communications and authentication within the limited onboard processing capacity of IoT devices.

FINDINGS & RECOMMENDATIONS

On-board Malware Detection: CISA should continue to track R&D efforts by NIST and industry to develop these technologies until the availability improves and becomes widely adopted by manufacturers.

Secure On-boarding Protocols: CISA should continue to monitor the development of secure on-boarding protocols by NIST to determine when they sufficiently mature to be required for CI system or component acquisitions.

Lightweight cryptography: CISA should continue to track NIST's evaluation of LWC standards and industry to develop this encryption technology until the availability improves, projected in 2 to 3 years.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
On-board Malware Detection	R&D				
Secure On-boarding Protocols	R&D				
Lightweight Cryptography	R&D				

IoT SECURITY

SMART BUILDING/CITY CYBER SITUATIONAL AWARENESS

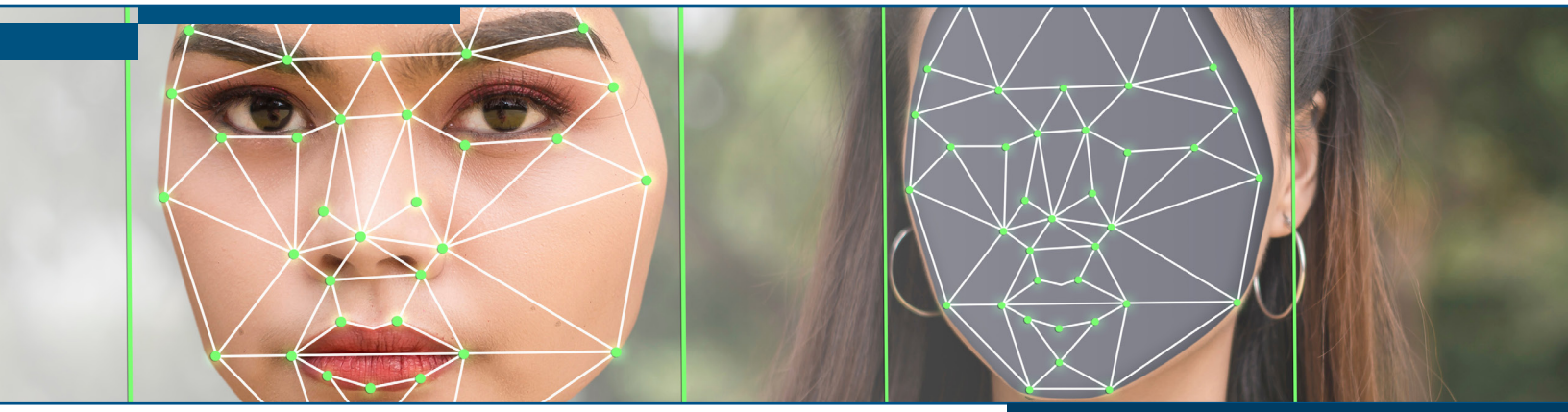
Smart Cities are municipalities that use information and communication technologies to increase operational efficiency and improve both the quality of government services and citizen welfare. City leaders have identified citizens safety and security as the top priority when implementing smart city technologies. To improve safety, operators, analysts, and first responders need to quickly understand the current scene, as well as emerging situations in and around the city. Smart cities need to use smart city enabling technologies to develop cyber situational awareness capabilities that help detect and respond to threats. These technologies include five tiers of the smart city cyber/physical technology architecture: Physical, Data, Enablers, Applications, Management, Partners, and Consumers. Each smart city service relies on one or more components of each architectural layer to operate safely and securely. Cyber situational awareness is developed by combining information from each component of each architectural layer to create and present an integrated description of the state of the smart city to provide decision makers with the information and incident analysis needed to address incidents as they unfold. Incident analysis may provide response recommendations, incident history, and automated responses. Incidents may be caused by cyber affects and human-made or natural events. Incident examples may include: a cyber-attack on traffic signals or public transportation, floods, or public gatherings. Smart city sensors and control devices are being deployed today. They include street sensors and cameras, smart meters, smartphones, water level gauges, and numerous other types of sensors.

FINDINGS & RECOMMENDATIONS

CISA should consider establishing test beds and partnerships to develop the concepts and techniques for developing situational awareness and incident response capabilities for smart city environments. Emphasis should be placed on applying smart city technologies that improve public safety and critical infrastructure security whose outputs can be leveraged and integrated to provide cyber situational awareness.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Smart Building/City Cyber Situational Awareness	Demo				

LARGE SCALE ANALYTICS
DEEPFAKE DETECTION



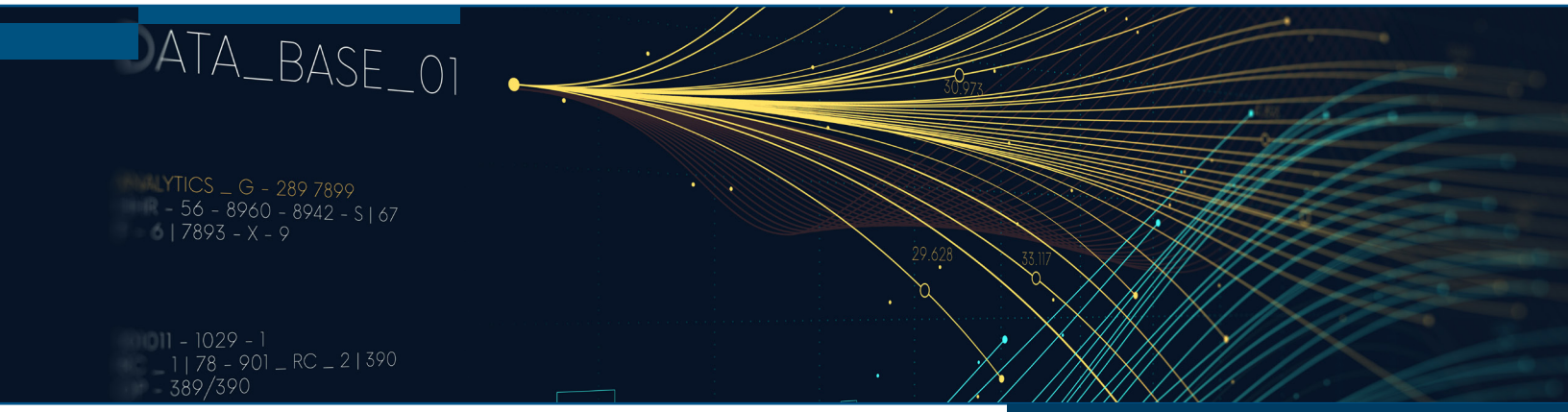
The use of Machine Learning (ML) to generate realistic fake images, videos, and audio known as "deepfakes" has been rising over the years and creates substantial threats to the fabric of our society and democracy. State of the art technology can realistically synthesize a person's voice using only seconds of their speech, as well as create images and video depicting people in situations where they were never present. These technologies are rapidly improving, much faster than research on developing technologies to detect fake speech, video, and images. The underlying technology responsible for video and image deepfakes are found in Generative Adversarial Networks (GAN), a class of ML framework pioneered by Ian Goodfellow and his colleagues in 2014. In this method, two neural networks (a generator and discriminator) compete against each other in a mini-max game to produce a model capable of generating new data with the same properties of the training set. The U.S. government recognizes the threat deepfake technology poses. The National Defense Authorization Act 2021 included the bi-partisan Deepfake Report Act as an amendment, which requires the DHS to conduct annual studies of deepfakes (i.e., digital content forgery). Detecting deepfakes requires a multi-stakeholder and multi-modal approach. Collaborative actions and collective techniques across legislative regulations, platform policies, technology intervention, and media literacy can provide effective and ethical countermeasures to mitigate malicious threats intended by deepfakes.

FINDINGS & RECOMMENDATIONS

CISA should demonstrate internally to further develop techniques, systems, and best practices to enable deepfake detection in acquired images. For example, CISA should consider collaborating with creators of recording technologies, to support the standardization of recording technologies that would require electronic devices to implement digital signatures in their hardware. With such a standard in place, received media could be authenticated, confirming it came from a device and has not been tampered.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Deepfake Detection	Demo				

LARGE SCALE ANALYTICS
PRIVACY ENHANCING TECHNOLOGY



Multiple privacy enhancing technologies (PETs) have emerged in recent years. Each one is at varying stages of maturity, with different applicability and use cases:

Homomorphic Encryption (HE): HE allows encrypted data to be processed while it remains encrypted, preserving confidentiality in cloud computing and other vulnerable environments. Current implementations of HE require high computation loadings, but research on hardware-based solutions show promise.

Multiparty Computation (MPC): MPC allows multiple parties to cooperate on joint computations without sharing the contributed data to others. Several implementations have proven worthwhile, but labor intensive.

Federated Learning (FL): FL is a machine learning development technique for statistical analysis or model training on decentralized data sets whose contents remain undisclosed. Any model (e.g., Naïve Bayes, Support Vector Machine) can be used. It requires a central server to coordinate the analysis among the decentralized data sets.

Differential Privacy (DP): DP is a data aggregation method that adds randomized "noise" to the data, allowing for a quantification of privacy risk. It is currently employed by industry and government, including the U.S. Census Bureau. There are no clear best practices or standards on the proper tradeoff between accuracy and privacy.

FINDINGS & RECOMMENDATIONS

CISA should continue to evaluate these technologies through R&D and demonstrations. These technologies are not interchangeable. Based on requirements and maturity, CISA should develop a general use case for each technology to help stakeholders refine their specific uses cases and choose the appropriate technologies for their cases

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Homomorphic Encryption	R&D				
Multiparty Computation	Demo				
Federated Learning	Demo				
Differential Privacy	Demo				

NETWORK SYSTEMS SECURITY

BORDER GATEWAY PROTOCOL (BGP) SECURITY

Border Gateway Protocol (BGP) is the protocol used globally by the independently managed Internet networks to exchange information about the route options for packets to traverse the Internet from source to destination. BGP was designed to enable adoption among a small and trusted set of initial network/Autonomous System (AS) operators. Trust was an assumption in the design of BGP, and this assumption led to protocol security weaknesses. Multiple BGP security protocols have been adopted by the Internet Engineering Task Force (IETF). However, BGP security can only be achieved when all, or most, of the AS operators implement the same protocols. A study of BGP security protocol deployments indicates when the top 100 AS operators/Internet service providers (ISPs) implement Route Origin Validation, the impact of malicious use of BGP can be mitigated or significantly reduced.

IETF has published standards designed to mitigate the BGP security weaknesses. In some (not all) cases, the standards require AS (ISPs and mobile network operators) operators to add technology to support new protocols. At this time, the technology needed is commercially available. The security risk impact factor addressed by BGP security is a reduction in effectiveness and efficiency of National Security and Emergency Preparedness (NS/EP) personnel communications. NS/EP personnel are not the only stakeholders affected. Vulnerabilities in BGP are used to attack critical infrastructure and other private entities for various malicious outcomes including ransom and hacktivism.

FINDINGS & RECOMMENDATIONS

CISA should work with the FCC and AS operators to encourage the adoption of BGP security protocols and any necessary implementation technology. The Federal Communications Commission (FCC) published a Notice of Inquiry, February 28, 2022, to collect public comments on the vulnerabilities and proposed approaches to improve the security of Internet routing, specifically BGP.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
BGP Security Protocol RFCs & Technology	Adopt				

NETWORK SYSTEMS SECURITY

SMALL & MEDIUM SIZED BUSINESS (SMB) PENETRATION TEST AUTOMATION TOOL

Penetration testing, or pen testing, is the set of tactics and techniques used to enumerate the vulnerabilities of an organization's IT infrastructure. Examples of the categories of vulnerabilities include system configuration, patching status, identity management and access control, network security, physical access control, and many others an adversary/criminal can exploit. Pen testing automation is also called Breach and Attack Simulation (BAS). The majority of small and medium businesses (SMBs) depend on a managed service provider to provide, plan, and implement a cybersecurity program. Therefore, any BAS system for SMBs should be designed for users with minimal or no technical cybersecurity knowledge. Currently, no BAS systems are available that meet this requirement. The security risk factors associated with SMB IT infrastructure include the entire range of IT infrastructure vulnerabilities (e.g., re-used passwords, unpatched software, and mis-configured network security). Successful exploitation of a vulnerability can create significant physical, economic, and personal safety impacts.

Tools exist that automate some aspects of pen testing. These tools require a prior knowledge of the technical characteristics and configurations of the IT infrastructure to be tested, and cybersecurity SMEs to operate the tools properly. Research continues to identify techniques to automate pen testing. Pen testing can be sub-categorized as either external testing (performed from outside of the IT infrastructure) and internal testing (performed from within the IT infrastructure).

FINDINGS & RECOMMENDATIONS

Given the potential effects resulting from attacks on SMBs in the SLTT and CI sectors, CISA should support R&D efforts to improve pen test automation in cybersecurity research organizations and industry. The payback is a reduced risk probability factor of successful cyber-attacks on CI and SLTT IT infrastructure operated by or supported by SMBs.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
SMB Penetration Test Automation Tool	R&D				

NETWORK SYSTEMS SECURITY

ZERO TRUST ARCHITECTURE (ZTA)

Zero Trust Architecture (ZTA) is a set of design concepts. The key concept is that instead of using perimeter defenses to protect a flat enterprise network, every access request to sensitive data is checked and connected only to those resources that are permitted by centrally controlled access policies. This change affects every aspect of enterprise IT design including users, devices, networks, applications, data, monitoring, and governance. Executive Order (EO) 14028 on Improving the Nation's Cybersecurity released on May 12, 2021, directs executive agencies to develop a plan to implement ZTA.

NIST SP 800-207 defines an architecture for ZTA that is considered the reference architecture for the federal government. CISA and others have also defined ZTA maturity models that provide metrics for assessing progress toward ZTA implementation. The National Cybersecurity Center of Excellence (NCCoE) at NIST is collaborating with industry partners to develop guidelines for implementing ZTA. The first phase of this project is nearly complete, and several other phases are planned. At the conclusion of the project, the NCCoE intends to document and make the reference implementation available for demonstration.

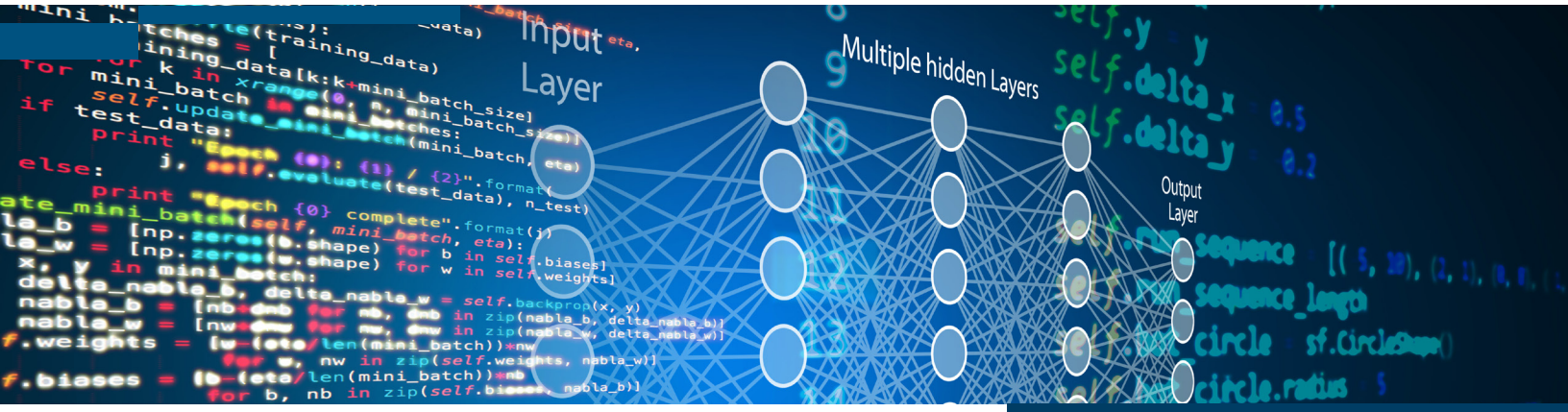
Even though much progress has been made by many agencies toward the implementation of ZTA, significant work is still needed to fully realize all tenets of ZTA across the federal enterprise.

FINDINGS & RECOMMENDATIONS

CISA should participate in NIST ZTA projects to contribute expertise and maintain awareness of the NIST guidance changes and lessons learned from proof-of-concepts. Areas for research include integration standards and continuous authentication.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
ZTA	R&D				

RESILIENT MACHINE LEARNING (ML) SYSTEMS



ML systems emulate the way a human learns. They can be more effective or efficient than humans in digesting large amounts of data, and quickly and accurately detecting patterns. ML systems are increasingly being used in cybersecurity and critical infrastructure (CI) applications for malware scanning; intrusion detection; facial and fingerprint recognition; Security Orchestration, Automation and Response (SOAR); and large-scale analytics. ML systems are vulnerable to attacks that exploit the design, training, and operation of these systems. These attacks include data poisoning attacks, where training data is tainted; evasion attacks, where input data is modified so the model incorrectly classifies it; and oracle attacks, where an adversary extracts data from the model using successive queries.

Researchers are developing techniques to prevent these attacks. Poisoning attacks can be mitigated by detecting or preventing the injection of bad data into the ML training data set, and evasion and oracle attacks can be mitigated by obscuring training data or making the models less sensitive to perturbations. NIST and DARPA are developing, and have recently released, test and evaluation frameworks intended to be used by ML system developers and acquisition programs to evaluate how ML systems respond to typical forms of attack.

FINDINGS & RECOMMENDATIONS

CISA should monitor the development of attack defenses and demonstrate the value of test and evaluation (T&E) frameworks

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Evasion & Oracle Attack Defenses	Monitor	Demo			
Data Poisoning Attack Defenses	Monitor	Demo			
ML Resilience Test & Eval Frameworks	Demo				

SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR) EFFECTIVENESS

SOAR technologies automate security actions using connections to security sensors and other technology platforms in (or connected to) an organization. SOAR technologies can be configured to execute playbooks or workflows that consist of a series of actions, including response actions (e.g., triage a list of alerts, quarantine a user session, run a vulnerability scan, open a ticket, update a signature, alert an analyst). In this manner, playbooks provide security organizations with a mechanism to automate processes (or portions of processes) that were previously manually conducted by security operations staff.

Orchestration is the integration and coordination of disparate security tools, platforms, and people to enable the best possible response to cyber security events. Orchestration is used to: 1) manage and coordinate the actions of multiple cyber defense analysts and tools so they operate seamlessly and rapidly in response to critical cyber threats; 2) manage and coordinate the gathering and proper distribution of critical cyber information to support incident response by ensuring the right people receive actionable information in a timely fashion; and 3) capture and define cyber defense processes and procedures so they can be standardized, shared, and utilized throughout the enterprise.

ML is presently incorporated into SOAR products to improve effectiveness and efficiency.

FINDINGS & RECOMMENDATIONS

CISA should adopt and encourage its stakeholders to adopt SOAR technologies using ML where repetitive analysis tasks and responses can be codified and automated. Utilizing ML within a SOAR platform may significantly improve staff effectiveness by identifying similar incidents and courses of action providing analysts recommendations that improve future responses and incident playbooks.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
ML & SOAR	Adopt				

SOFTWARE ASSURANCE & VULNERABILITY MANAGEMENT

SOFTWARE INTEGRITY TESTING

Software integrity testing is validating that software provides the intended capability performance, and only the intended capability performance. There is a critical need to field capabilities that enable software examinations at scale to test for known functionality, software previously examined (labelling), and label validations. Software integrity validation results and labeling can later be incorporated into the development of a software bill of materials (SBOM) that provides verifiable attestation a software's capabilities and/or vulnerabilities fall into a bounded set of known or intended behavior.

The following capabilities are critical to enable Software Integrity Testing: (1) automated software functionality testing; (2) unique software labels that correlate to a verifiable set of tested attributes; (3) automated label Identification at scale and remotely to discover and verify deployed software beyond a formal test environment; (4) tracking the composition of, and provenance of, every component of a software product; (5) cryptographic code signing and a validation infrastructure sufficient for a heterogenous mix of commercial-off-the-shelf (COTS), open-source, and custom development; and 6) SBOMs to track every code component and modification.

Test automation tools are a crucial component in the DevOps toolchain. The current test automation trends increasingly apply ML to offer advanced capabilities for test optimization, intelligent test generation, execution, and reporting.

FINDINGS & RECOMMENDATIONS

Software integrity testing is essential to measure the safety, security, and reliability of software being employed to support critical operations and functions. CISA should Demo capabilities to enable software integrity testing at scale, and encourage FSLTT and CI stake-holders to implement, as appropriate through best practices.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Software Integrity Testing	Demo				

SOFTWARE ASSURANCE & VULNERABILITY MANAGEMENT

SOFTWARE BILL OF MATERIALS (SBOM)

Software Bill of Materials (SBOMs) are a record of the components comprising a software product (open source and proprietary code) provided to anyone building, procuring, and/or operating the software product. Third-party components are a known systemic risk to software systems. SBOMs are a security measure under development which would provide all participants in the software supply chain a listing of the constituent components of software products. The listing can be referenced to determine appropriate actions if a vulnerability or update emerges for any component. SBOMs also contain supply chain relationships of various components used in building a product. These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or access restricted. SBOMs can create transparency within the software supply chain to better document and understand system risk factors, support development of mitigations, and drive better software development practices. To establish software pedigree and provenance, an SBOM at minimum should include:

- Software part numbers and versions
- Libraries and frameworks used in development
- Tool chain used, and
- Languages and versions used in development.

FINDINGS & RECOMMENDATIONS

Establishing consensus around the use and common standards for developing an SBOM is critical to demonstrating value and encouraging stakeholder adoption. A standardized, machine-readable SBOM can provide critical decision support to defenders. CISA should demonstrate SBOM capabilities to encourage FSLTT and CI stakeholders to integrate SBOM into their software development and procurement practices.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
SBOM	Demo				

SOFTWARE ASSURANCE & VULNERABILITY MANAGEMENT

LATE LIFE CYCLE BINARY REDUCTION

Modern software is exceedingly complex and bloated. Current software development practices and frameworks encourage this state (e.g., object-oriented programming, libraries, deprecated code, layers of abstraction). In addition to increasing software complexity, there are often many blocks of code within complex systems of software (including the layers of libraries) that are redundant or perform similar functions. Many blocks perform extraneous, seldom-used, or never-used functionality. Feature creep, device-specific optimizations, and attempts to support multiple different architectures all contribute to software bloat.

The Office of Naval Research Total Platform Cyber Protection (TPCP) program developed a late life cycle binary reduction capability. This capability addresses four key objectives: (1) feature removal; (2) de-layer and de-bloat; (3) harden the security; and (4) verify and validate. The techniques used to achieve these objectives include: (1) binary reverse engineering; (2) feature-to-code association; (3) dependency identification; (4) assisted removal of undesired features; (5) functionality-preserving transformation of desired features for aggressive code reduction; (6) retrofitting security constructs potentially trimmed in previous reductions; and (7) automated validation in situ to ensure transformation results are robust and secure. These late-stage customizations are independent of a developer's selection of environment, libraries, number of libraries used, and compiler.

FINDINGS & RECOMMENDATIONS

CISA should pursue demonstrations internally for late life cycle binary reduction to determine its utility and risk to operations. DoD success in real-world system application of these techniques, and a successful demonstration, should lead to adoption of these techniques to reduce the attack surface of CI.

TPCP also supports overall cybersecurity improvements because the approach reduces the protocol attack surface and vulnerabilities in unnecessary code. It also supports, and is dependent on, strong, automated verification and validation.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Late Life Cycle Binary Reduction	Adopt				

MISSION CRITICAL SERVICES (MCS) ON CELLULAR NETWORK

Mission Critical Services (MCS) has grown beyond Mission Critical Voice (MCV) or Push to Talk (PTT) to include Mission Critical Video (MCVideo), Mission Critical Data (MCData), and Mission Critical SMS. All these services are offered through FirstNet, the public safety network, run by AT&T, created in the wake of the 9/11 attacks on U.S. soil. While FirstNet is built on the open commercial 3GPP-based standards, there is disagreement among the mobile network operators regarding what constitutes interoperability. Namely, whether the public safety network is intended to be a single, nationwide network, or intended to be a "network of networks." This confusion has contributed to limited interoperability between AT&T FirstNet and public safety network offerings of other mobile network operators. A key dependency to enable the maximum benefits of MCS over cellular is integration with Land Mobile Radio (LMR) systems and other telecommunication carriers (cellular and ISP). As standards are still under development for these capabilities, interoperability challenges among communication equipment components will continue to exist. Additional capabilities may also be required before first responders accept cellular services as full replacements for LMR systems. For example, high audio quality and volume, coupled with the need for voice recognition, impose constraints on the type, quality, and location of speakers.

FINDINGS & RECOMMENDATIONS

CISA should recommend FSLTT and CI operators adopt this technology to address MCS on cellular networks. In addition, CISA should continue participating in the 3GPP specifications development; coordinate with other agencies such as NSA or NIST that are participating in 3GPP MCS specifications development, as well as government and private sector first responder communities of interest to collect requirements; and influence standards for the products and services that enable MCS on cellular networks.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
MCVideo	Adopt				
MCData	Adopt				

NEXT GENERATION NETWORK PRIORITY SERVICES (NGN-PS)

Next Generation Network (NGN) is the term used to describe the packet switched IP based network supporting voice and data communications (including text, video, graphics, images, and information communications), and enabling converged communication on a single device. NGN-Priority Services (NGN-PS) will provide prioritized FSLTT data communications services for both mobile (wireless) and ISP networks. Various priority levels are assigned to pre-authorized FSLTT users/devices through a DHS Emergency Communications Division (ECD) priority and pre-emption approval process. NGN-PS also refers to Multimedia Priority Services (MPS) including SMS and multimedia services (MMS) provided by mobile network operators. Ultimately, much of the National Security and Emergency Preparedness (NS/EP) voice and data communications will migrate to NGN-PS as indicated in DHS ECD NGN-PS acquisition project reports. Inter-MPS provider quality of service (QoS) enables end to end priority handling of NS/EP communications.

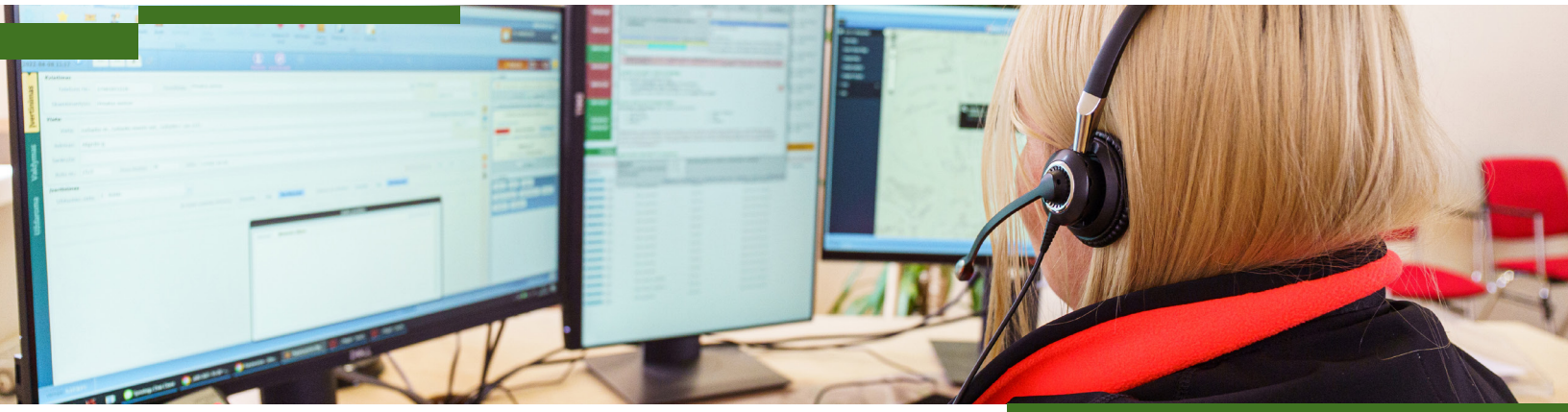
FINDINGS & RECOMMENDATIONS

CISA should monitor and participate with other government organizations in the work groups developing the 3GPP priority and pre-emption specifications. The four other technologies (VPN service with proper QoS, Inter-MPS provider QoS, Government network peering, and Ad-hoc Mobile Networking) have the potential to support NGN-PS today and should be demonstrated in pilots or testbeds to illustrate their value to NS/EP and FSLTT organizations for providing priority services.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Inter-MPS Provider QoS	Demo				
VPN Service with Proper Qos	Demo				
Government Network Peering	Demo				
3GPP Priority & Pre-emption Specs	Monitor	Demo			
Ad-hoc Mobile Networking	Demo				

EMERGENCY COMMS CENTER IMPROVEMENTS

COMPUTER AIDED DISPATCH (CAD) INTEROPERABILITY



States and localities are stronger when they know of, and can rely upon, a fabric of shared situational awareness and resources that fosters resilience and interoperability beyond any individual legal jurisdiction. Situational awareness is more beneficial to society when it is based upon the natural geography and relationships that sustain population centers. Dispatchers, call takers, and 911 operators use CAD systems to prioritize and record incident calls, identify the status and location of responders in the field, and effectively dispatch responder personnel. Emergency responders in the field can receive messages initiated by CAD systems via their Mobile Data Terminals, radios, and cell phones. CAD systems may also interface with a Geographic Information System, an Automatic Vehicle Location system, a caller identification system, logging recorders, and various databases.

CAD-to-CAD interoperability solutions are commercially available and currently fielded by some local and regional jurisdictions across the country, capable of integration via Application Programing Interfaces. However, integration is hampered by a lack of industry standardization to ensure consistent and reliable data exchange. An evolving solution landscape creates confusion for potential adopters. From a cybersecurity perspective, the additional data exchanges from CAD-to-CAD interoperability introduce new controllable risks such as privacy, need-to-know, and new threat vectors from an expanded data exchange footprint and associated distributed systems.

FINDINGS & RECOMMENDATIONS

CISA should encourage adoption of CAD Interoperability among National Security and Emergency Preparedness stakeholders. The initial Emergency Incident Data Document (EIDD) and Emergency Incident Data Object (EIDO) interoperability base standards need to be completed. CAD interoperability and conformance testing to base standards (EIDD and EIDO) as well as industry support for the commercialization roadmap development in the relevant environment up to TRL 7-8 needs to be completed.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
CAD Interoperability	Adopt				

EMERGENCY COMMS CENTER IMPROVEMENTS

CYBERSECURITY CENTERS

The Next Generation 911 (NG911) system, which operates on an IP platform, enables interconnection among a wide range of public and private networks; such as wireless, the Internet, and analog phone networks. The NG911 system enhances the capabilities of today's legacy 911 network -- allowing compatibility with more types of communication systems and data, providing greater situational awareness to dispatchers and emergency responders, and establishing a level of resiliency not previously possible. NG911 will allow Emergency Communications Centers to accept and process a range of information from first responders and the public, including text, images, video, and voice calls.

A central cybersecurity intrusion detection and prevention service (IDPS) has been proposed by the FCC to support the national, regional, and local jurisdiction's Public Safety Answering Points (PSAPs)/Emergency Communications Centers (ECCs) and other emergency communications services (ECS) and systems. This central cybersecurity service provider is referred to as an Emergency Communications Cybersecurity Center (EC3). The goal of the center is to provide cybersecurity IDPS capabilities beyond individual jurisdictions' capabilities and develop nation-wide situational awareness to improve response to incidents. The EC3 concept at this time is limited to IDPS capabilities and does not include security enhancements that address the increasing threats that come from multimedia sharing and connectivity becoming available with the Next Generation 911 (NG911) system.

FINDINGS & RECOMMENDATIONS

CISA ECD is investigating establishing a Cyber Resilient 911 capability. The capability could cover material and non-material solutions. Potential needs have been identified to include education and training, cybersecurity risk management, and stakeholder engagement. Capability development could include cybersecurity as a service and establishing an operations center. CISA should continue to research and develop capabilities consistent with these needs including the use of AI to improve cyber security capabilities and more advanced tools for risk management.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Emergency Comms Cybersecurity Center	R&D				

EMERGENCY COMMS CENTER IMPROVEMENTS

ENHANCED CYBERSECURITY SERVICES

The Next Generation 911 system (NG911) will allow Emergency Communications Centers (ECCs) to accept and process a range of information from first responders and the public, including text, images, video, and voice calls. Whether through the Emergency Communications Cybersecurity Center (EC3) concept, or in-house, ECCs should address the increasing threats that come from multimedia sharing and connectivity. ECC cybersecurity should integrate Machine Learning (ML), large-scale analytics, deep fake detection, and image processing capabilities to address content-based attacks.

ML can detect suspicious or anomalous events by learning what constitutes normal event behavior, comparing new events to the learned behavior, and adapting accordingly. ML will need to conduct image processing (such as object recognition, and image reconstruction and enhancement) to improve the quality and utility of processed imagery, as well as identify optimal sources from potentially numerous inputs for an incident. Image processing via ML will also need to implement deepfake detection capabilities to counter misinformation efforts designed to deceive First Responders and misuse limited resources.

FINDINGS & RECOMMENDATIONS

CISA should work to refine the EC3 concept to include ML capabilities to address multimedia content-based attacks. Real-time AI/ML video analytics technologies must be created to detect emergencies and support public safety response to emergencies. Additionally, AI/ML can be used to detect RF anomalies and perform distributed NG911 AI/ML predictive analysis at the wireless service provider mobile-edge-computing (MEC) and the ESInet logical connection with the PSAP/ECC.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Image Processing for ECCs/PSAPs	Adopt				
Deepfake Detection for ECCs/PSAPs	Demo				
ML & Large-Scale Analytics for ECCs/ PSAPs	R&D				

EMERGENCY COMMS CENTER IMPROVEMENTS

INFORMATION EXCHANGE

Information sharing across organizational boundaries requires a level of trust between participants. An organization providing sensitive information needs assurance the recipient of the information will handle it appropriately. An organization receiving information needs to have some level of confidence in the integrity and validity of the information provided.

In addition to these security and information handling considerations, information sharing also requires interoperability among partners. Depending on how information is shared, interoperability might require the use of standard protocols, data formats, cryptography, and messaging channels. The Trustmark Framework is a technology construct developed to facilitate information sharing by providing assurance to interacting parties that their partners comply with relevant security and interoperability requirements. A Trustmark is a machine-readable statement of conformance of an organization or system to a specific set of identity trust and/or interoperability requirements.

A Trustmark provides participating stakeholders with assurance of compliance to information security requirements and that access to information is limited to pre-defined need to know requirements. A Trustmark can also be used to verify a user's identity and the identity assurance level for that identity.

FINDINGS & RECOMMENDATIONS

The transition of the Trustmark Framework beyond the proof-of-concept phase into production use depends on the availability of software tools to be able to define, issue, and validate a Trustmark for the Trustmark Providers, Trustmark Recipients, and other actors in the Trustmark Framework. CISA should continue to support the R&D efforts with S&T, with the goal of funding the technological support for Trustmark adoption

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
ECC Information Exchange	R&D				

EMERGENCY COMMS CENTER IMPROVEMENTS

PRECISION LOCATION & NEXT GENERATION 911 (NG911) HIGHER LOCATION RESOLUTION

Precise location is the term used for technologies that provide location accuracy within one meter for horizontal and vertical (X, Y, and Z axis) location reporting indoors or outdoors. DHS Components and first responders are interested in utilizing precise location capabilities to improve location tracking for improved situational awareness, user safety, and tracking team members during incidents for common operational picture (COP) use. The Federal Communications Commission (FCC) regulates the cellular industry location reporting requirements for calls to 911/emergency centers. The FCC has issued rules for nationwide cellular service providers that establish 911 call indoor location reporting accuracy at +/- 50 meters horizontal (X/Y axis or dispatchable location) and +/- 3 meters vertical (Z axis). The deadline for all cellular carriers to provide vertical indoor location reporting is 2026. At this time, the FCC has not issued rules requiring precise (+/- 1 meter) location reporting

Current Global Positioning System (GPS)-based smartphones provide 4.5 meter location accuracy for outdoor location detection, with continuing improvements in power consumption, cost, and anti-jamming occurring in commercial industry R&D. Indoor location detection continues to evolve as mobile network operators and handset manufacturers improve technology to meet the FCC requirements identified above.

FINDINGS & RECOMMENDATIONS

CISA should work with precise location vendors and the S&T Office of Interoperable Communications (OIC) to adopt and determine the feasibility of accelerating deployment of precise location. S&T and the National Aeronautics and Space Administration's (NASA's) Jet Propulsion Laboratory (JPL) developed a system called Precision Outdoor and Indoor Navigation and Tracking for Emergency Responders (POINTER) to provide high precision indoor and outdoor location detection. POINTER is planned for commercialization in 2022.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Precise Location & NG911 Higher Location Resolution	Adopt				

RESILIENT COMMUNICATIONS

MOBILE SIGNAL JAMMER

CISA stakeholders, especially first responders, depend on radio communications systems to conduct their missions. These systems are vulnerable to jamming attacks by adversaries who seek to interfere or degrade the ability of first responders to execute their missions. Many methods have been developed and are routinely used to improve the performance of radio systems such as spread spectrum modulation, directional high-gain antennas, low noise receivers, and cognitive radios. These improvements have limitations and do not completely meet the mission need to enable first responders to communicate in the presence of interference or jamming signals.

Significant progress has been made in using quantum sensing techniques to use atomic sensors to detect electric fields, Rydberg electric field sensors. These sensors can be tuned to very precise frequencies to reduce the effects of noise and interference on a desired signal such as transmission of voice or data from a first responder. Advantages of atomic electric field sensors include resistance to interference, self-interference mitigation, broad tunability, small sensor head size, and resilience from intense field events. Because of the potential advantages, active research is being conducted by many large R&D organizations such as NASA, NIST, DARPA, Army Research Lab (ARL), and DHS S&T as well as European and Chinese labs. In practice, these sensors could be used as an alternative radio receiver front end, as a radio spectrum usage sensor, or as a jammer direction detector.

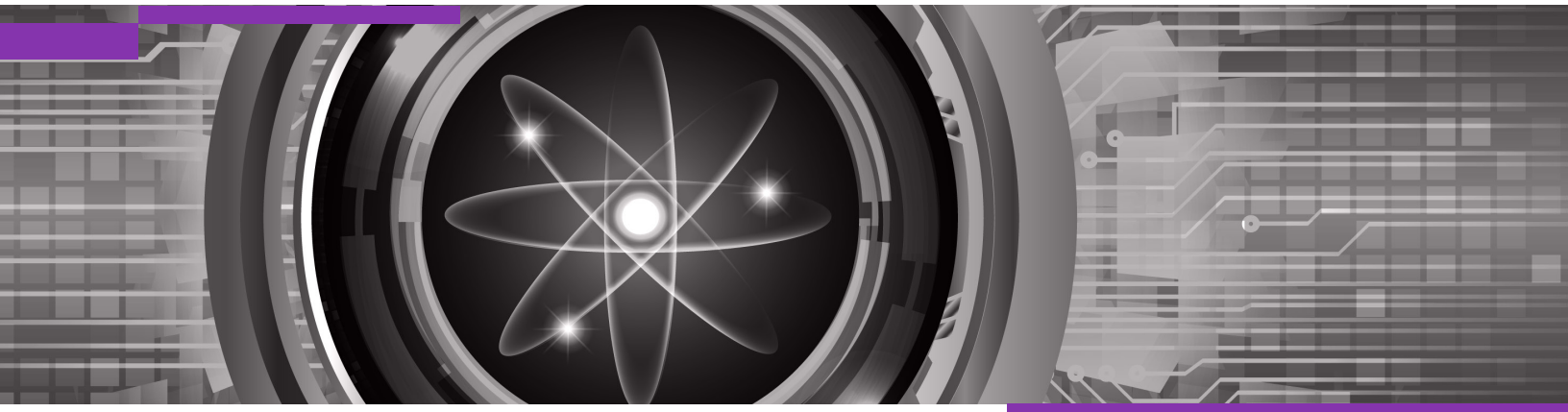
FINDINGS & RECOMMENDATIONS

CISA should monitor the development of Rydberg electric field sensors technologies until availability is more mature. It is anticipated that this technology will be ready for field demonstration in 3-4 years.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Rydberg Atom Electric Field Sensor	Monitor	Monitor	Demo		

AUTHORITATIVE TIME SOURCE

LOW-COST ACCURATE ATOMIC BACKUP CLOCK



An authoritative time source is a single source of time (at a given local site) by which events can be time-stamped, correlated, and synchronized, at a national and international level, both for local and external use. Such a time source is necessary for efficient and effective cybersecurity operations (e.g., Security Orchestration, Automation, and Response; Security Information and Event Management; and forensic analyses). Additionally, functions and services executed at the local site depend on this time source for events such as timestamping financial transactions, controlling industrial plant operations, and synchronizing transmission media for communications. The authoritative time source is synchronized to Coordinated Universal Time (UTC) with an accuracy determined by the functions and services conducted at the local site (often at the microsecond level). Global Positioning System (GPS) is used broadly as a time source and has become the de facto national timing reference due to its ease of integration, precision, low cost, and wide availability. GPS, via the authoritative time source, provides the timing for functions executed within critical infrastructure (CI). However, GPS signals have low signal strength at the receiver and can be disrupted via various mechanisms (e.g., natural and unintentional interference, spoofing, and jamming). Given the dependence on GPS, any disruption to the time source represents a major risk to communications systems, as well as many other CI sectors. The ubiquitous need for a highly accurate timing source indicates a demand for economically viable low-cost accurate atomic backup clocks. These atomic oscillators are used to provide accurate time during periods when GPS disruptions are present (e.g., spoofing or interference).

FINDINGS & RECOMMENDATIONS

CISA should maintain knowledge of DARPA and NIST progress in R&D efforts to develop low-cost alternatives. Once the capability is ready for a technology transfer to vendors, then CISA may elect to demonstrate the capability in pilots with various CI partners (or others).

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Low-Cost Accurate Atomic Backup Clock	R&D				

EMP & GMD ACTIVE MITIGATIONS

An electromagnetic pulse (EMP) is a burst of electromagnetic energy that has the potential to negatively affect technology systems on Earth and in space. A high-altitude EMP (HEMP) is a type of human-made EMP that occurs when a nuclear device is detonated at approximately 40 kilometers or more above the surface of the Earth. An EMP is caused by a nuclear or nonnuclear device, while HEMP is only caused by a nuclear device. A geomagnetic disturbance (GMD) is a natural EMP due to a temporary disturbance of the Earth's magnetic field resulting from a Coronal Mass Ejection (CME). GMD can be caused by a solar storm, or another naturally occurring phenomenon, and a CME can generate a GMD if the CME event impacts the Earth with sufficient strength and at the proper angle.

Both HEMPs and GMDs can affect large geographic areas. The effects of any of these electromagnetic disturbances are of national concern for all CI sectors, including destruction of unprotected electronics in communications systems and adverse effects on the electric grid. An important aspect of EMP-GMD events is that due to cascading effects, not all devices in a system or network need to be affected to result in significant service blackouts. Even though a small number of devices may be affected by the event, other devices depend on the affected ones, which results in entire systems or geographic areas being affected. All CI sectors are subject to such cascading failures. These effects can be mitigated via passive or active technologies. Passive technologies (e.g., resistors and capacitors installed on transmission lines, surge arresters, Faraday cages, and grounding) are installed in infrastructure at all times, and were recommended as Adopt in STRv4, while active technologies are switched into place when an event is detected.

FINDINGS & RECOMMENDATIONS

Given the low Availability score, in the near term, CISA should track industry R&D efforts until the Availability score is higher.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
Active EMP/GMD Mitigation Technologies & Techniques	R&D				

QUANTUM RESISTANT ENCRYPTION

Quantum Resistant Encryption (QRE) is the next generation of encryption algorithms designed to be secure against both quantum and classical computers yet remain compatible with existing communications protocols and networks. In July 2022, NIST announced four candidate QRE algorithms for standardization. NIST is expected to finalize these standards in 2024. QRE is a requirement for security when cryptography relevant quantum computers (CRQCs) are realized. CRQCs will be the first generation of quantum computers able to reliably implement the algorithms necessary to break the asymmetric encryption used in today's public key cryptography or infrastructure.

Crypto agile encryption (CAE) is the recommended approach for transitioning to QRE. CAE is an enhancement to enable future encryption algorithm changes without operational disruptions, such as those expected when implementing the new NIST algorithms.

The security risks a CRQC creates include the loss of confidentiality and integrity of data at rest and data in transit. They also include the loss of integrity of the authentication mechanisms used for access and permission decisions on virtually all enterprise and public Internet applications and services, as well as cellular communications. Also, integrity of software distribution techniques is reduced or eliminated due to the use of asymmetric encryption for these checks.

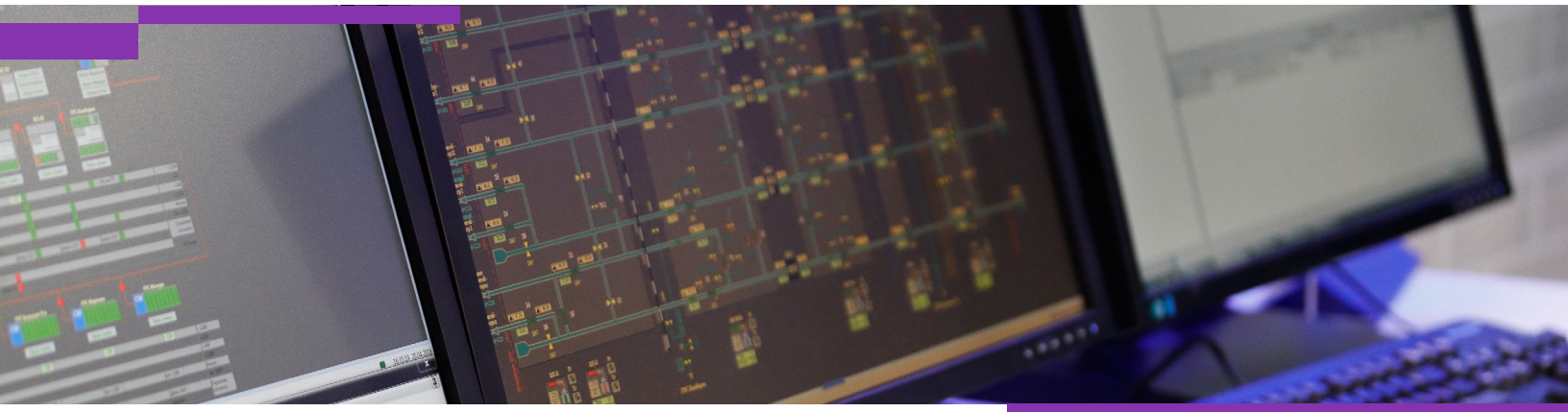
FINDINGS & RECOMMENDATIONS

CISA should track NIST standards and industry R&D efforts to develop QRE. Given the time required to transition (up to a decade), the transition planning should begin now. CISA should recommend to acquisition organizations within CISA, FSLTT entities, and critical infrastructure operators, that they start discussions and approaches to include QRE requirements in acquisitions without delay. Government, CIs, and industry need to acknowledge the coming era of CRQC to maximize the probability that the capabilities will be available when needed.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
CAE	Demo				

RISK REDUCTION VIA MODELING

SUPERVISORY CONTROL & DATA ACQUISITION (SCADA) CYBERATTACK SIMULATION



Cyber ranges provide the capability to rapidly emulate networks, as well as adversary threat activities, for the purposes of performing realistic cybersecurity testing and supporting training and mission rehearsal exercises. Large variations in environments, operating systems, applications, network topologies, Internet Protocol address configurations, router configurations, and user policies exist across various enterprises. Well designed and resourced cyber ranges address these challenges -- giving the developers, integrators, and operators a realistic, large-scale cyber test environment tailored to specific test requirements: reliably, rapidly, and repeatedly.

To accurately simulate industrial control system/Supervisory Control and Data Acquisition (ICS/SCADA) environments, a DHS cyber range capability should leverage both virtualized and/or simulated capabilities and emphasize the inclusion of real-world ICS components via hardware in the loop simulation to better understand real-world system performance and impacts. CISA Cybersecurity Division (CSD) uses the Control Environment Lab Resources (CELR) test range to execute operations-focused research on the cybersecurity of ICS. The CELR environment currently has three different ICS environments under development: Chemical Manufacturing, Electrical Distribution and Transmission, and Building Management.

FINDINGS & RECOMMENDATIONS

DHS has a need to expand usage and availability of cyber range capabilities that include both IT and OT components which mirror architectures employed within critical infrastructure environments. CISA should continue to invest in the ICS/SCADA cyber range capability, providing greater fidelity simulations of IT and OT environments, threat emulation, accessibility of range resources to partners, and the ability to support multiple events at multiple security levels.

Technology	<2 Years	2-3 Years	3-4 Years	4-5 Years	>5 Years
SCADA Cyberattack Simulation	Adopt				

CISRR FOCUS AREAS
POTENTIAL ALIGNMENT TO DHS S&T R&D RESEARCH PROJECTS

	Critical Infrastructure Security Research and Resilience Focus Areas (CISRR)				
	FOCUS 1: Special Event Risk Assessments Rating Planning Tools	**FOCUS 2:** EMP & GMD Resilience Capabilities	**FOCUS 3:** PNT Capabilities	**FOCUS 4:** Public Safety & Violence Prevention/Soft Target Security	**FOCUS 5:** Security Testing Capabilities for Telco, equipment, ICS, and Open-Source Software
DHS S&T R&D Projects					
CAD-to-CAD Interoperability					■
Countering Foreign Influence Survey					■
Cyber Analytics & Platform Capabilities Phase II	■				
Cyber-Resilient Public Safety Infrastructure					■
CISA Advanced Analytics Platform for Machine Learning (CAP-M)					■
EMP & GMD Resiliency		■			
Evaluation of Soft Target Security & Prevention				■	
Event Security Decision Support Tools	■			■	
Harmful Narrative Alignment Patterns in Sweden & U.S.					■
ICS Control Environment Lab Resource (CELR), Auto & Retail Testbeds					■
PNT			■		
Secure & Resilient Mobile Network Infrastructure (SRMNI)					■
Software Assurance Supply Chain					■
Trustmark					■

CISRR FOCUS AREAS
ALIGNMENT TO STR COMMUNICATIONS DOMAIN CAPABILITY DEMANDS

	Critical Infrastructure Security Research and Resilience Focus Areas (CISRR)				
Cybersecurity Technologies	FOCUS AREA 1	FOCUS AREA 2	FOCUS AREA 3	FOCUS AREA 4	FOCUS AREA 5
ICS Security					
Asset Detection for ICS					■
RHIMES Technology					■
ICS Patch Automation					■
ML Enabled SCADA IDS Anomaly Detection					■
Integrated Physical & Cyber SIEM					■
IoT Security					
On-Board Malware Detection					
Secure On-Boarding Protocols					■
Lightweight Cryptography					■
Smart Building/Cyber Situational Awareness					
Large Scale Analytics					
Deepfake Detection				■	
Homomorphic Encryption	■				
Multiparty Computation	■				
Federated Learning	■				
Differential Privacy	■				
Network Systems Security					
BGP Security					■
SMB Cybersecurity Pen Test Automation Tool					
ZTA					■
Resilient ML Systems					
Evasion & Oracle Attack Defenses					
Data Poisoning Attack Defenses					
ML Resilience Test & Evaluation Frameworks					
SOAR Effectiveness					
ML & SOAR					
Software Assurance & Vulnerability Management					
Software Integrity Testing					■
SBOM					■
Late Lifecycle Binary Reduction					■

CISRR FOCUS AREAS
ALIGNMENT TO STR COMMUNICATIONS DOMAIN CAPABILITY DEMANDS

	Critical Infrastructure Security Research and Resilience Focus Areas (CISRR)				
Communications Technologies	FOCUS AREA 1	FOCUS AREA 2	FOCUS AREA 3	FOCUS AREA 4	FOCUS AREA 5
MCS on Cellular Network					
Mission Critical Video (MCVideo)					■
Mission Critical Data (MCData)					■
NGN-PS					
VPN Service with Proper QoS					■
Inter-MPS Provider QoS					■
Government Network Peering					■
3GPP Priority & Pre-emption Specifications					■
Ad-hoc Mobile Networking					■
Emergency Communications Center Improvements					
CAD Interoperability					■
Emergency Communications Cybersecurity Centers					■
Image Processing for ECCs/PSAPs					■
Deepfake Detection for ECCs/PSAPs					■
ML & Large-Scale Analytics for ECC/PSAPs					■
ECC Information Exchange					■
Precise Location & NG911 Higher Location Resolution					■
Resilient Communications					
Rydberg Atom Electric Field Sensor					■

CISRR FOCUS AREAS ALIGNMENT TO
STR CRITICAL ENABLERS DOMAIN CAPABILITY DEMANDS

Critical Enablers					
Authoritative Time Source					
Low-Cost Accurate Atomic Backup Clock			■		
EMP & GMD Mitigations					
Active EMP/GMD Mitigation Technologies & Techniques		■			
Quantum Resistant Encryption					
Crypto Agile Encryption					■
Risk Reduction via Modeling					
SCADA Cyberattack Simulation					■

Science and Technology

R&D PROJECT MAPPING
DHS SCIENCE AND TECHNOLOGY R&D RESEARCH PROJECTS

	Capability Demand Area														
	Cybersecuriy							Emergency Communications				Critical Enablers			
	ICS Security	IoT Security	Large Scale Analytics	Network Systems Security & Res	Resilient ML Systems	SOAR Effectiveness	SW Assurance & VM	MCS on Cellular Network	NGN-PS	ECC Improvements	Resilient Communications	Authoritative Time Source	EMP & GMD Mitigations	Quantum Resistant	Risk Reduction via Modeling
CAD-to-CAD Interoperability										■					
Countering Foreign Influence Survey			■												
Cyber Analytics & Platform Capabilities Phase II			■		■	■									■
Cyber-Resilient Public Safety Infrastructure									■	■					
CISA Advanced Analytics Platform for Machine Learning (CAP-M)	■	■	■	■	■	■									
EMP & GMD Resiliency													■		
Evaluation of Soft Target Security & Prevention															■
Event Security Decision Support Tools															■
Harmful Narrative Alignment Patterns in Sweden & U.S.			■												
ICS Control Environment Lab Resource (CELR), Auto & Retail Testbeds	■														
PNT												■			
Secure & Resilient Mobile Network Infrastructure (SRMNI)								■							
Software Assurance Supply Chain							■								
Trustmark										■					

R&D PROJECT MAPPING
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA) PART 1

	Capability Demand Area														
	Cybersecuriy							Emergency Communications				Critical Enablers			
	ICS Security	IoT Security	Large Scale Analytics	Network Systems Security & Res	Resilient ML Systems	SOAR Effectiveness	SW Assurance & VM	MCS on Cellular Network	NGN-PS	ECC Improvements	Resilient Communications	Authoritative Time Source	EMP & GMD Mitigations	Quantum Resistant	Risk Reduction via Modeling
Active Social Engineering Defense			■												
All Together Now												■			
Assured Micropatching	■														
Atomic Clock with Enhanced Stability												■			
Automated Rapid Certification of Software							■								
Automated Implementation of Secure Silicon							■								
Brandeis			■		■										
Competency-Aware ML						■									
Computers & Humans Exploring Software Security							■								
Configuration Security (ConSec)							■								
Cooperative Secure Learning			■												
Cyber Assured Systems Engineering	■														
Cyber-Hunting at Scale					■	■									
Data Protection in Virtual Environments			■												
Explainable AI			■			■									
Guaranteeing AI Robustness Against Deception					■										
Harnessing Autonomy for Countering Cyberadversary Systems			■			■									
Hybrid AI to Protect Integrity of Open-Source Code			■												

R&D PROJECT MAPPING

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA) PART 2

	Capability Demand Area														
	Cybersecuriy							Emergency Communications				Critical Enablers			
	ICS Security	IoT Security	Large Scale Analytics	Network Systems Security & Res	Resilient ML Systems	SOAR Effectiveness	SW Assurance & VM	MCS on Cellular Network	NGN-PS	ECC Improvements	Resilient Communications	Authoritative Time Source	EMP & GMD Mitigations	Quantum Resistant	Risk Reduction via Modeling
In the Moment			■							■					
Influence Campaign Awareness & Sensemaking			■												
Learning with Less Labeling					■										
Lifelong Learning Machines					■										
Machine Common Sense					■										
Open, Programmable, Secure 5G															
Quantum Apertures											■				
Rapid Attack Detection, Isolation, & Characterization Systems	■					■									
Resilient Anonymous Communication for Everyone			■												
Reverse Engineering of Deceptions					■										
Robust Optical Clock Network												■			
Securing Information for Encrypted Verification & Evaluation			■												
Semantic Forensics			■												
Signature Mgt using Operational Knowledge & Environments															■
Symbiotic Design for Cyber Physical Systems					■										
System Security Integration through Hardware & Firmware							■								
Verified Security & Performance Enhancement of Large Legacy SW							■								

U.S. DEPARTMENT OF ENERGY

R&D PROJECT MAPPING
DEPARTMENT OF ENERGY R&D PROJECTS

	Capability Demand Area														
	Cybersecuriy							Emergency Communications				Critical Enablers			
	ICS Security	IoT Security	Large Scale Analytics	Network Systems Security & Res	Resilient ML Systems	SOAR Effectiveness	SW Assurance & VM	MCS on Cellular Network	NGN-PS	ECC Improvements	Resilient Communications	Authoritative Time Source	EMP & GMD Mitigations	Quantum Resistant	Risk Reduction via Modeling
A Radiation Tolerant Clock Generator for the CMS Endcap Timing Layer Readout Chip	■														
An Intelligent Distributed Ledger Construction Algorithm for IoT		■			■										
AI for Energy systems Cybersecurity					■	■									
Enabling Computation on Sensitive Data in International Safeguard with Privacy-Preserving Encryption Techniques			■												
Implementing Cybersecurity for Distributed Wind: An Exercise in ICS Security Application	■														
Prioritizing ICS Beachhead Systems for Cyber Vulnerability Testing	■														
Real-Time GIS Programming & Geocomputation										■					
Universal Utility Data Exchange (UUDEX) Functional Design Requirements – Rev 1						■									

National Science Foundation

R&D PROJECT MAPPING
NATIONAL SCIENCE FOUNDATION (NSF) R&D PROJECTS PART 1

	Capability Demand Area														
	Cybersecuriy							Emergency Communications				Critical Enablers			
	ICS Security	IoT Security	Large Scale Analytics	Network Systems Security & Res	Resilient ML Systems	SOAR Effectiveness	SW Assurance & VM	MCS on Cellular Network	NGN-PS	ECC Improvements	Resilient Communications	Authoritative Time Source	EMP & GMD Mitigations	Quantum Resistant	Risk Reduction via Modeling
AI-Enabled Recovery and Assurance of Semiconductor IP from SEM Images	■														
Artificial Intelligence Assisted Malware Analysis					■	■									
Concealing Side-Channels in Real-Time Schedulers						■									
Data-driven Attack and Defense Modeling for Cyber-Physical Systems	■														
Enabling Trustworthy Upgrades of Machine-Learning Intensive Cyber-Physical Systems	■					■									
Enhancing Security for Modern Software Programming Cyberinfrastructure							■								
Foundations for IoT Cloud Security		■													
Going Beyond Linear Models for Attack Detection and Defense in Control Systems	■														
Integrated Circuit Cloaking against Reverse Engineering	■														
Low Earth Orbit Navigation System (LEONS) - The Ground Network												■			

National Science Foundation

R&D PROJECT MAPPING
NATIONAL SCIENCE FOUNDATION (NSF) R&D PROJECTS PART 2

	Capability Demand Area														
	Cybersecuriy							Emergency Communications				Critical Enablers			
	ICS Security	IoT Security	Large Scale Analytics	Network Systems Security & Res	Resilient ML Systems	SOAR Effectiveness	SW Assurance & VM	MCS on Cellular Network	NGN-PS	ECC Improvements	Resilient Communications	Authoritative Time Source	EMP & GMD Mitigations	Quantum Resistant	Risk Reduction via Modeling
Multi-Layer Dynamic Strategic Decision-Making for Integrated Cyber-Physical Energy Systems Sec and Res	■														
Post-Training Deep Neural Networks Certification Against Backdoor Data Poisoning Attacks					■										
Re-configurable, Source-Language-Agnostic Decompilation for Binary Programs							■								
Towards Attack-Resilient Cyber-Physical Smart Grids: Moving Target Defense for Data Integrity Attack Detection, Identification, and Mitigation	■														
Towards Label Enrichment and Refinement to Harden Learning-based Security Defenses					■										
Towards Reliable Operating Systems through Scalable Control and Data-Flow Analysis							■								

ARTIFICIAL INTELLIGENCE (AI) AUTONOMOUS PERFORMER

One of the major challenges we face now, and into the foreseeable future, is the availability of human resources to meet the demand for computer and information technology (IT) skills. This demand for skilled human resources parallels substantial evolutionary advancements in artificial intelligence (AI) capabilities. The potential of AI as a means of augmenting the computer and IT workforce is of great interest as it could significantly optimize functions within a range of occupations, and AI could fine-tune the specific skills needed by the human workforce. Clear trends in AI services have emerged that are clustered around uses such as analytics and intelligence, content creation and curation, and personal services. Of particular interest are advanced chatbots in use today such as Google Assistant, Amazon Alexa, Apple Siri, Microsoft Cortana, and Replika AI. Each chatbot brings its unique capabilities and features such as holding conversations with users, providing recommendations based on the user's preferences, and in some cases, even performing tasks on behalf of the user.

In the future, it is envisioned that AI autonomous performers will emerge that can perform tasks associated with a specific occupational role typically performed by humans. Whatever role AI serves, some aspect of the AI autonomous performer activities will likely require interacting with humans to solve complex problems. An AI autonomous performer should be able to complete tasks virtually, and it should be able to learn and adapt to new situations as they arise. The AI autonomous performer will likely need to be able to communicate with humans to receive instructions and feedback. Additionally, it may need to be able to work with other types of AI to complete more complex tasks or task pipelines (as in the case for an AI assembler who forms a product or service from AI orchestrator activities without specific direction by a human).

The use of AI as a member of the workforce will most likely require new ways of thinking about what an organization is, how an organization is composed, what is the right balance between humans and AI organizational members, and how to trust AI performers to act autonomously (particularly in roles that affect human life). It is conceivable that in the future if, and when, AI autonomous performers are developed for cyber defense, adversaries will develop AI autonomous performers for cyber-attack roles. This event will open an entirely new paradigm of AI-to-AI engagements; the implications of which are challenging to predict.

CISA IN THE METAVERSE

CISA is at the forefront of understanding and mitigating the risks to the increasingly interconnected mesh of cyber-physical systems; the agency has released a Cybersecurity and Physical Security Convergence Guide. This reference highlights the vulnerabilities introduced by interconnected systems and potential consequences of cyber threats to real world systems. In the metaverse, people, and more specifically individuals, become the vulnerability. The metaverse will likely lower the bar for malicious actors by readily providing the means and the opportunity to conduct malicious attacks against people. It potentially expands the attack surface available to nefarious actors, increases the risk of physical harm to persons, and further obfuscates and conceals cyber actors. Futurists speculate that virtual copies of real places, and novel and known items will be indistinguishable from the real world. The metaverse will be used to universalize experiences, conduct commerce, build communities, and more. We will experience the metaverse as augmented reality in real-world every-day important use cases such as navigation aids, informational labels, safety warnings and the like, delivered through glasses or goggles, gloves, earphones, and other wearables.

With the advent of this new reality, we can no longer manage cyber, physical, and people risks through separate lenses. Each of these dimensions presents unique vulnerabilities and impacts to privacy and security which the metaverse both magnifies and obscures. In particular, the metaverse magnifies risks associated with identity, spying, and social engineering.

CISA supports the management of cyber and physical risks by sharing information on cyber threats, vulnerabilities, and mitigations with stakeholders; coordinating the national response to cyber threats; and operating infrastructure which provides cyber defense for federal civilian agencies. CISA will require capabilities to rapidly identify emerging threats that originate and operate in the metaverse, communicate these risks to stakeholders through existing means, and in the metaverse, respond to security incidents in the metaverse, and build new capabilities which defend stakeholders from malicious actors in the metaverse.

DEFINITIONS FOR CAPABILITY DEMANDS

FINDINGS AND RECOMMENDATIONS TABLES

ADOPT: CISA concludes that industry and/or government (internal CISA and/or FSLTT) should adopt, or encourage adoption of, a technology or capability. The Adopt phase is focused on operationalizing a new technology, such as developing and utilizing deployment best practices, infrastructure integration and delivery, operational procedures, external relationship management, and human resource development.

DEMONSTRATE: These items 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, testbed, 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.

R&D: These items show significant value potential for improving operations or mission effectiveness and are currently, or should be, planned for R&D investment (e.g., lab breadboards or experimentation, R&D funding for applied research). The R&D phase is designed to "stabilize" an emerging technology, which may include experimentation, hiring of engineering resources, and developing a strategy for integrating an emerging technology into operational capabilities. Items recommended for R&D have moved beyond the conceptual to the growth phase, where the emerging technology must be exploited to further understand the development and integration challenges, value proposition, and risk factors.

MONITOR: These items are identified as worth considering with the goal of understanding how they might affect CISA and stakeholder operations and/or improve mission effectiveness, to justify further R&D or other investment in the future. Elements of these technologies may be conceptual in nature and require evolution prior to further investment, experimentation, and potentially adoption. The Monitor phase is focused on identifying those technologies that show potential for significant value proposition and capacity to significantly alter or disrupt how essential mission functions are executed in the future. Monitor items may have uncertainty around the risks the technology poses due to maturity, state of R&D, and complexity.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

2023-2027

STRATEGIC TECHNOLOGY ROADMAP

VERSION 5

PUBLICATION: NOVEMBER 2022 | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY