Federal Cybersecurity Research and Development Strategic Plan

Prepared by the

CYBER SECURITY AND INFORMATION ASSURANCE
INTERAGENCY WORKING GROUP

SUBCOMMITTEE ON NETWORKING & INFORMATION TECHNOLOGY
RESEARCH & DEVELOPMENT

COMMITTEE ON SCIENCE & TECHNOLOGY ENTERPRISE

of the

NATIONAL SCIENCE & TECHNOLOGY COUNCIL

DECEMBER 2019

About the National Science and Technology Council

The National Science and Technology Council (NSTC) is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development enterprise. A primary objective of the NSTC is to ensure that science and technology policy decisions and programs are consistent with the President's stated goals. The NSTC prepares research and development strategies that are coordinated across Federal agencies aimed at accomplishing multiple national goals. The work of the NSTC is organized under committees that oversee subcommittees and working groups focused on different aspects of science and technology. More information is available at https://www.whitehouse.gov/ostp/nstc.

About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 to provide the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics. OSTP leads interagency science and technology policy coordination efforts, assists the Office of Management and Budget with an annual review and analysis of Federal research and development in budgets, and serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. More information is available at https://www.whitehouse.gov/ostp.

About the Subcommittee on Networking & Information Technology Research & Development

The Networking and Information Technology Research and Development (NITRD) Program is the Nation's primary source of federally funded work on pioneering information technologies (IT) in computing, networking, and software. The NITRD Subcommittee of the NSTC Committee on Science and Technology Enterprise guides the multiagency NITRD Program in its work to provide the research and development (R&D) foundations for ensuring continued U.S. technological leadership and meeting the needs of the Nation for advanced IT. The National Coordination Office (NCO) supports the NITRD Subcommittee and the Interagency Working Groups (IWGs) that report to it. More information is available at https://www.nitrd.gov/about/.

About the Cyber Security and Information Assurance Interagency Working Group

The Cyber Security and Information Assurance (CSIA) IWG of the NITRD Subcommittee is focused on advancing solutions to many pressing cybersecurity issues through coordination of Federal cybersecurity R&D investments and activities, including developing joint research strategies and engaging academia and industry through workshops and other outreach activities. CSIA IWG member agencies focus on R&D to deter, protect, detect, and respond to actions that compromise or threaten to compromise the confidentiality, integrity, or availability of computer- and network-based systems. Such systems provide critical functions in every sector of the economy, including in national defense, homeland security, and other vital Federal missions. More information is available at https://www.nitrd.gov/groups/csia/.

About This Document

This 2019 Federal Cybersecurity Research and Development Strategic Plan supersedes the 2016 Federal Cybersecurity Research and Development Strategic Plan. The Plan aims to coordinate and guide federally funded R&D in cybersecurity, including development of consensus-based standards and best practices. The Plan identifies four interrelated defensive capabilities (deter, protect, detect, and respond) and six priority areas for cybersecurity R&D (artificial intelligence, quantum information science, trustworthy distributed digital infrastructure, privacy, secure hardware and software, and education and workforce development) as the focusing structure for Federal cybersecurity R&D activities and investments to benefit the Nation.

Copyright Information

National Science & Technology Council

Chair

Kelvin Droegemeier, Director, Office of Science and Technology Policy (OSTP)

Staff

Chloé Kontos, Executive Director, National Science and Technology Council (NSTC)

Committee on Science & Technology Enterprise

Co-Chairs

France Córdova, Director, National Science Foundation (NSF)

Walter G. Copan, Director, National Institute of Standards and Technology (NIST)

Paul M. Dabbar, Under Secretary for Science, Department of Energy (DOE)

Subcommittee on Networking & Information Technology Research & Development

Co-Chairs

Kamie Roberts, Director, National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD)

Erwin Gianchandani, Deputy Assistant Director, Directorate for Computer Information Science and Engineering, NSF

Executive Secretary

Nekeia Butler, NITRD NCO

Cyber Security & Information Assurance Interagency Working Group

Co-Chairs

Jeremy Epstein, Deputy Division Director, Computer and Network Systems, NSF

William Newhouse, Deputy Director, National Initiative for Cybersecurity Education, NIST

Staff

Tomas Vagoun, Technical Coordinator, NITRD NCO

Strategic Plan Development Task Group

Nina Amla, NSF

Shannon Beck, NSF

Sushil Birla, U.S. Nuclear Regulatory Commission

Dan Clouse, National Security Agency

Dan Cosley, NSF

Jeremy Epstein, NSF

Fowad Muneer, DOE

Brendon Gibson, Department of Homeland Security (DHS) (contractor)

Jonathan Heiner, Air Force Research Laboratory

Erin Kenneally, DHS

James Kirby, Naval Research Laboratory

Sandip Kundu, NSF

Paul Lopata, Office of the Secretary of Defense (OSD)

William Newhouse, NIST

Tristan Nguyen, Air Force Office of Scientific Research

Victor Piotrowski, NSF

Indrajit Ray, NSF

Vincent Sritapan, DHS

Cynthia Stanley, OSD

Martin Stanley, DHS

Tomas Vagoun, NITRD NCO

William Vesey, OSD (contractor)

and reviewers in a number of agencies in the NITRD Program

Table of Contents

Executive Summary

Information technology (IT) provides exceptional benefits to society. However, the more society relies on IT, the greater the potential disruption and destruction that adversaries can create via malicious cyber activities. Advances in cybersecurity are urgently needed to preserve the Internet's social and economic benefits—as well as the security of the Nation and its online commercial and public infrastructure—by thwarting adversaries and strengthening public trust in cyber systems.

The *Cybersecurity Enhancement Act of 2014* (Public Law 113-274) requires the National Science and Technology Council and the Networking and Information Technology Research and Development Program to develop, maintain, and update every four years a cybersecurity research and development (R&D) strategic plan to guide the overall direction of federally funded R&D in cybersecurity. This strategic plan (this "Plan") fulfills this mandate and updates the 2016 *Federal Cybersecurity Research and Development Strategic Plan*. This Plan also addresses priorities established by the 2018 *National Cyber Strategy of the United States of America,* including both its domestic and foreign policy priorities, and by the Administration's FY 2021 Research and Development Budget Priorities Memorandum.

The Plan identifies the following goals for cybersecurity R&D:

- Understand human aspects of cybersecurity
- Provide effective and efficient risk management
- Develop effective and efficient methods for deterring and countering malicious cyber activities
- Develop integrated safety-security-privacy framework and methodologies
- Improve systems development and operation for sustainable security

To realize the goal of a secure cyberspace, the Plan carries forward the essential concepts from the 2016 *Federal Cybersecurity Research and Development Strategic Plan*, including the framework of four interdependent defensive capabilities:

- Deter
- Protect
- Detect
- Respond

To advance the priorities and objectives of the 2018 *National Cyber Strategy of the United States of America* and the Administration's FY 2021 Research and Development Budget Priorities Memorandum, the Plan outlines research objectives in the following priority areas:

- Artificial Intelligence
- Quantum Information Science
- Trustworthy Distributed Digital Infrastructure
- Privacy
- Secure Hardware and Software
- Education and Workforce Development

Advancements in the defensive capabilities and priority areas critically depend on progress in human aspects, research infrastructure, risk management, scientific foundations, and transition to practice.

The Plan closes with identifying roles in cybersecurity R&D for the Federal Government, industry, and academia and with recommendations for supporting activities. Implementing this Plan and these recommendations will create science and technology for cybersecurity that effectively and efficiently sustain a trustworthy cyberspace to support the Nation's prosperity and security well into the future.

Introduction

Information technology (IT) continues to be woven into every aspect of modern life. Emerging technologies of the 21st century, such as high-speed mobile networking and smart cities, promise that cyberspace will continue to offer exceptional benefits to society. However, the more society relies on IT, the greater the potential disruption and destruction that adversaries can create via malicious cyber activities. Today, U.S. intellectual property is being stolen, critical infrastructure is at risk, commercial and government computer systems are being compromised, and consumers are worried about their privacy. As currently deployed, the Internet places both public and private sectors at a disadvantage versus cyber criminals and other malicious adversaries. Advances in cybersecurity are urgently needed to preserve the Internet's societal and economic benefits by establishing a position of assurance and trust for cyber systems and professionals. Strategic R&D investments by the Federal Government can contribute to advances in cybersecurity, help secure the cyberspace, and ultimately, strengthen the U.S. economy.

In September 2018, the President released the *National Cyber Strategy of the United States of America*, outlining how the Administration will, "(1) defend the homeland by protecting networks, systems, functions, and data; (2) promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserve peace and security by strengthening the ability of the United States—in concert with allies and partners—to deter and, if necessary, punish those who use cyber tools for malicious purposes; and (4) expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet."[1] Through its National Cyber Strategy and FY 2021 Research and Development Budget Priorities Memorandum,[2] this Administration has established the following areas as priorities for cybersecurity and related R&D:

- Maintaining military superiority supported by advanced cyber capabilities derived from new computing and technology paradigms.
- Improving the security and resilience of the Nation's critical infrastructure.
- Maintaining leadership in artificial intelligence (AI) and quantum information science (QIS), and advancing a secure computational infrastructure and ecosystem.[3]
- Developing advanced communications networks and R&D to secure networks and manage wireless spectrum.
- Maintaining leadership in semiconductor design, including assured access to advanced microelectronics.
- Prioritizing initiatives that provide education and job opportunities in science, technology, engineering, mathematics, and computer science to a wide spectrum of American students and workers.

In support of these priorities, this 2019 *Federal Cybersecurity Research and Development Strategic Plan* provides guidance and defines priorities for Federal agencies that conduct or sponsor R&D in cybersecurity.

This Plan updates the 2016 *Federal Cybersecurity Research and Development Strategic Plan*[4] as required

[1] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, p. I.

[2] https://www.whitehouse.gov/wp-content/uploads/2019/08/FY-21-RD-Budget-Priorities.pdf (Memorandum M-19-25).

[3] NSTC. *National Strategic Computing 2019 Update: Enabling the Future of Computing* (November 2019); https://www.whitehouse.gov/wp-content/uploads/2019/11/National-Strategic-Computing-Initiative-Update-2019.pdf.

[4] https://www.nitrd.gov/pubs/2016-Federal-Cybersecurity-Research-and-Development-Strategic-Plan.pdf

by the *Cybersecurity Enhancement Act of 2014* (Public Law 113-274).[5] This law requires the National Science and Technology Council (NSTC) and the Networking and Information Technology Research and Development (NITRD) Program to develop, maintain, and update every four years a cybersecurity R&D strategic plan to guide the overall direction of federally funded R&D in cybersecurity.

This Plan was developed by a task group of subject-matter experts from the NSTC and the NITRD Program under the leadership of the White House Office of Science and Technology Policy. The task group also issued a Federal Request for Information through NITRD to provide industry, academia, and the public an opportunity to offer input to this Plan.[6] Responses to this Request for Information are posted on the NITRD website.[7]

This 2019 Plan carries forward essential concepts and framing from the 2016 *Federal Cybersecurity Research and Development Strategic Plan*:

- Effective cybersecurity requires maturing capabilities founded upon four defensive elements: Deter, Protect, Detect, and Respond (this was previously *Adapt*; however, *Respond* is a more comprehensive approach that includes *Adapt*).
- Science and technology (S&T) advances are needed to counter adversaries' asymmetrical advantages in cyberspace with proactive risk management, through sustainably secure systems development and operation, and via effective and efficient deterrence of malicious cyber activities.
- A strong focus is required on evidence-driven S&T for cybersecurity; evidence of efficacy and efficiency is needed to guide cybersecurity R&D and to improve cybersecurity practices.
- Advances in the following areas are critical to successful cybersecurity R&D: human aspects, research infrastructure, risk management, scientific foundations, and transition to practice.

The following key updates and new priorities are put forth by this 2019 Plan:

- People—users who are affected by computing and communication systems—must be included in the realm that needs to be protected by cybersecurity, in addition to systems and data.
- Frameworks and methodologies are needed that will enable developers to reason across and manage safety, security, resiliency, and privacy requirements holistically and concurrently.
- Efficient adaptation, countering, and recovery capabilities are needed to engender an effective Respond capability.
- Focused and coordinated R&D investments are needed in the cybersecurity aspects of these priority areas: artificial intelligence, quantum information science, trustworthy distributed digital infrastructure, privacy, secure hardware and software, and education and workforce development.

Cybersecurity R&D is a shared responsibility, with essential roles for government, industry, and academia. Government funds long-term, high-risk research and performs mission-specific R&D. Industry funds near-term research and transitions successful research into commercial products. This document lays out a research agenda for federally funded R&D carried out by government agencies and the U.S. R&D enterprise, informed by interactions with industry and academia.

[5] https://congress.gov/113/plaws/publ274/PLAW-113publ274.pdf

[6] https://www.federalregister.gov/documents/2018/11/13/2018-24668/request-for-information-on-update-to-the-2016-federal-cybersecurity-research-and-development

[7] https://www.nitrd.gov/nitrdgroups/index.php?title=CSIA-RFI-Responses-2019

Strategic Framing

This Plan focuses on thwarting malicious cyber activities and campaigns by developing S&T to support four defensive elements: Deter, Protect, Detect, and Respond. This strategy is driven by evidence-based evaluations and measurements of the efficacy and efficiency of cybersecurity S&T solutions. The solutions are effective if they achieve the desired security result; they are efficient when the measured units of benefit are greater than the minimized units of cost. Along with an investment in technology solutions, the Plan highlights the importance of investments in a diverse workforce of cyber professionals who can design and implement suitable cybersecurity measures as well as manage risk.

Cybersecurity Context

Cybersecurity must be understood as a multifaceted domain where a variety of social, technical, economic, and legal goals, actors, and processes interact. Solutions for improving cybersecurity need to be designed and evaluated in this multidisciplinary context. This Plan makes the following key observations about the cybersecurity domain:

Adversaries. Adversaries will perform malicious cyber activities if they perceive that the potential benefits outweigh their expended effort and probable consequences.

Defenders. Defenders must thwart malicious cyber activities against valuable and critical systems while technologies and threats are continually evolving.

Users. Users will circumvent cybersecurity practices that they perceive to be irrelevant, ineffective, inefficient, or overly burdensome.

Technology. Because technology connects the physical and cyber worlds, the risks and benefits of the two worlds are interconnected.

Dual-use. Many security technologies can be used for either offensive or defensive purposes.

Policy impact. National policies such as patents, regulations, or export controls can have significant impact on both research and the transition of research to practice.

Challenges

A fundamental research goal for cybersecurity is to make it less onerous while seeking to provide more effective protections. This challenge can be met by developing a deeper understanding of how to evaluate the quality of cybersecurity (including the assessment of the cyber risk), how to leverage cybersecurity mechanisms to support privacy needs, and how to manage tradeoffs between applying cybersecurity while maintaining delivery of vital services. To accomplish the vision of a trustworthy cyberspace and effective cybersecurity practices, priority should be given to developing solutions to the following goals:

Better understanding of human aspects: Today, “cybersecurity” is characterized too narrowly as the practice of protecting computers, networks, data, and the resulting IT systems. This characterization needs to be expanded to explicitly include the sociotechnical issues and the roles of humans as developers, defenders, users, and adversaries and to elevate human-oriented issues to be among the priorities for cybersecurity R&D. The human aspects goal also focuses on ensuring that end-users and computer professionals can understand and make effective security decisions, and that systems and policies account for their abilities, needs, and expectations.

Effective and efficient organizational risk management: Organizations need an understanding of the range of vulnerabilities and threats in cyberspace and how it applies to them. This involves evidence-based risk management, which is the process of identifying, assessing, and responding to risk, including the development of effective and measurable controls. Organizations must have access to evidence of the efficacy and efficiency of these controls as well as be prepared to consider the human aspects with respect to users, developers, operators, defenders, and adversaries.

Effective and efficient deterrence and countering of malicious cyber activities: Techniques are needed that can discourage malicious cyber activities by increasing costs and risks and lowering gains for adversaries. Active forms of deterrence that utilize appropriate countermeasures to reduce the operational effectiveness of malicious cyber activities are also needed—that is, actions or techniques that reduce threats, eliminate or prevent attacks, or minimize the harm they can cause.

Integrated safety-security-privacy framework: Many operational systems being developed today (e.g., autonomous vehicles) require that safety, security, resiliency, and privacy requirements be managed concurrently. However, frameworks do not yet exist that allow holistic integration of such requirements. Frameworks and methodologies are needed that will enable designers and developers to reason across all domains concurrently.

Sustainably secure systems: There is an acute need for design and implementation of software, firmware, and hardware that are highly resistant to malicious cyber activities, along with development of effective, measurable technical and nontechnical security controls that consider human behavior as well as the economic drivers associated with cyberspace.

Approach

This Plan provides a framework of four interrelated defensive elements to realize cybersecurity goals; they are defined as follows:

Deter: The ability to discourage malicious cyber activities by increasing the costs to, diminishing the spoils of, and increasing the risks and uncertainty for potential adversaries.

Protect: The ability of components, systems, users, and critical infrastructure to efficiently resist malicious cyber activities, and to ensure confidentiality, integrity, availability, and accountability.

Detect: The ability to efficiently detect, and even anticipate, adversary decisions and activities, given that perfect security is not possible and that systems should be assumed to be vulnerable to malicious cyber activities.

Respond: The ability of defenders, defenses, and infrastructure to dynamically react to malicious cyber activities by efficiently adapting to disruption, countering the malicious activities, recovering from damage, maintaining operations while completing restoration, and adjusting to thwart similar future activities.

These four elements are similar but not identical to the five core functions in the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.[8] Whereas the five NIST core functions (Identify, Protect, Detect, Respond, Recover) are geared toward operational cybersecurity risk management, this Plan is intended to guide cybersecurity R&D. The main

[8] https://doi.org/10.6028/NIST.CSWP.04162018

difference is that the Identify function and Deter element do not have exact complements in the two approaches. However, the differences do not introduce any incompatibility between these efforts.

While this Plan identifies the need for R&D to develop effective countering techniques, such techniques are intended to provide defensive capabilities. R&D for offensive cyber operations is out of scope for this Plan.

Figure 1 shows how the Plan's four defensive elements aim to thwart malicious cyber activities and campaigns and the value of continuous outcomes-driven improvements in efficacy and efficiency.

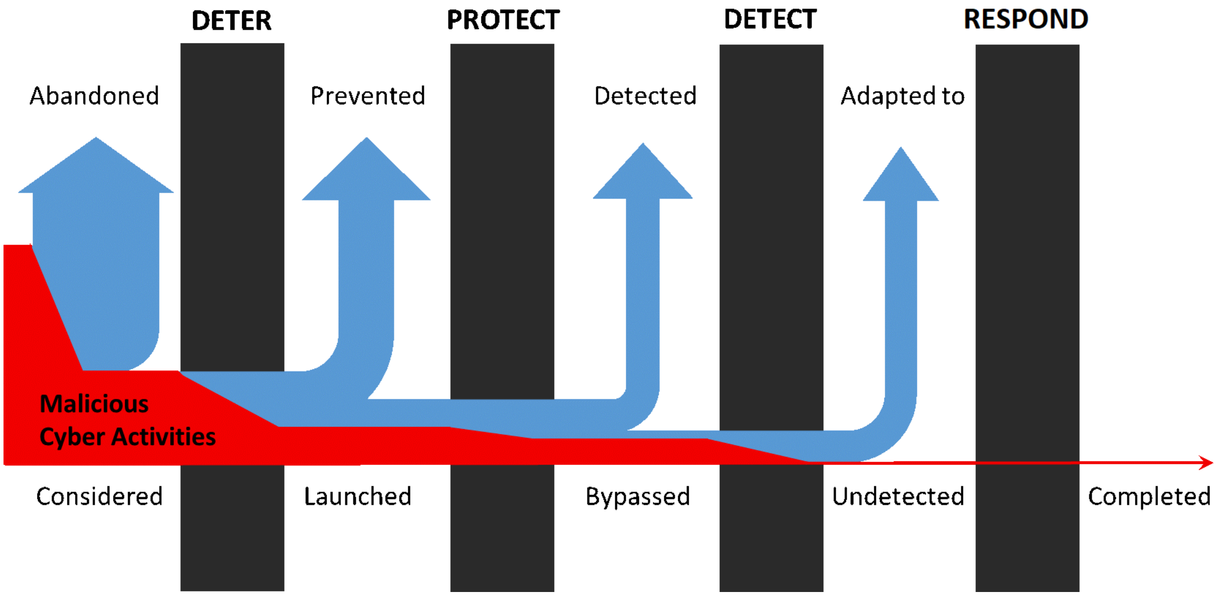

Figure 1. Continuously strengthening the four interrelated defensive elements improves success in thwarting malicious cyber activities overall.

The Defensive Elements

The value created by computing and networks will continue to be subverted by those seeking illicit gains. IT systems should be assumed to be vulnerable to malicious cyber activities, and perfect security is not possible. Security should be viewed as a flexible, ongoing process of self-evaluation and informed actions of adjusting and responding to threats as they evolve. The cybersecurity framing of Deter, Protect, Detect, and Respond addresses the full range of cybersecurity needs, and by doing so, it provides a structure for coordinating research and focusing on shared goals. This section describes each of the defensive elements.

Deter

The most effective way to secure a system from cyber threats is by deterring malicious cyber activities before they can compromise the system or the enterprise. Deterrence, in the broad sense used by this Plan, requires increasing the level of effort that adversaries must apply to achieve their objectives and increasing the possible negative consequences for them from their actions. If adversaries judge that the likely costs of malicious activities, including risks of prosecution or sanctions, are greater than their expected benefits, they are more likely to be deterred from attempting the activities. Increasing both the required level of effort and the negative consequences for adversaries is needed for successful deterrence. Deterrence through threats of retaliation (e.g., prosecution and sanctions) alone has not been effective against most malicious cyber activities due to current limitations with attribution of cyber attacks and prosecuting across jurisdictions.

Challenges

Deterrence requires effective, multipronged defenses that increase the number and types of resources an adversary must have. A successful cyber defense has many facets, ranging from the appropriate technological solutions (e.g., designing secure software, hardware, and operating systems), to network protocols and access controls, to human factors such as safe data handling by users. In this manner, effective deterrence relies on the other three defensive elements—Protect, Detect, and Respond—to increase the costs and decrease the benefits to adversaries of their malicious cyber activities.

Deterrence also requires successful attribution of cyber attacks to specific offenders to dissuade them from pursuing cyber attacks. However, identifying the origins of individual malicious actions in cyberspace can be difficult, because the actors are often in different jurisdictions than the systems they attempt to breach, and they operate through proxies and other anonymizing procedures. Improving attribution will require progress in effectively collecting and sharing activity indicators across organizations and jurisdictions. A related challenge is developing forensic techniques that are robust enough to preserve evidence such that it is suitable for use in legal proceedings while also bolstering immediate detection and cyber analytical abilities.

To meet these challenges, new technologies are needed to measure and verify the ability of an enterprise to thwart adversary efforts and to ensure that law enforcement, government agencies, and system and network owners can successfully attribute malicious activities to their sources. Examples follow of the needed capabilities:

Modeling attackers, defenders, and users. Effective models of the actors in cybersecurity are critical to properly assessing attackers' risks, costs, and capabilities. The Critical Dependencies, Human Aspects, section of this Plan gives a wide range of considerations for these models. In the context of deterrence, key factors are modeling attacker effort (i.e., money, time, or computational cost), effectiveness, and risks, given the characteristics and capabilities of the defenders and users.

Providing effective and timely attribution. Accurate attribution of malicious cyber activities to their sources opens a broad range of response options, such as sanctions or prosecution.

Supporting robust investigations. Effective investigative tools for law enforcement create the basis for collecting the evidence required for successful prosecution of cyber adversaries.

Sharing information for attribution. Effective mechanisms for sharing attribution information must be developed and must support investigations that cross international or domestic law enforcement jurisdictions.

Protect

The second defensive element, Protect, focuses on creating systems and networks that are highly resistant to malicious cyber activities through assurance-based engineering practices that will simultaneously protect a system and supply the verifiable evidence needed to support its assurance case.

Challenges

Limiting Vulnerabilities

There are five essential approaches needed to produce software, hardware, or firmware with fewer defects that present security vulnerabilities, as described below:

Design for security. In many cases, security vulnerabilities in a system are present from the start. To avoid systemic security vulnerabilities, system architects must begin with accurate threat models and a robust understanding of the intended applications. Further, security tools, policies, and systems must operate as part of larger sociotechnical systems. This demands design attention to interoperability, maintainability, and evolvability in the context of other technologies, and to how these tools can be adopted by and adapted to the human and organizational contexts in which they will be deployed.

Build secure. Implementation errors can undermine the security of well-designed components. Although common vulnerabilities such as buffer overflows and memory leaks are well understood by most developers, they remain difficult to eliminate. Existing tools and practices that prevent developers from creating specific types of security vulnerabilities are imperfect and inefficient. To reduce common product vulnerabilities, tools and practices for software and hardware development are needed that significantly improve developer productivity and operational system performance.

Verify security. Even when products are designed for security and are built to be robust, implementation errors may creep in during system development. In addition to undergoing functional testing, components should be subjected to rigorous security analysis throughout the development process. Because adversaries use static analysis tools and fuzzing tools to find previously unknown ("zero-day") software vulnerabilities, rigorous application of these tools should be used to identify and eliminate vulnerabilities before a product goes to market.

Maintain security. Inevitably, even software that is well-designed, implemented by knowledgeable developers with good tools, and subjected to comprehensive security testing still will have defects. When errors are identified, the software must be updated. The mechanisms used to update software can unintentionally introduce vulnerabilities instead of eliminating them. Building in secure mechanisms for updating software or firmware is essential to securing products throughout their lifecycles.

Verify authenticity. The four approaches listed above offer the potential to dramatically reduce the number of vulnerabilities in hardware and software, but only if users deploy authentic, unaltered products. Objective measures for supply-chain assurance are needed to increase an organization's ability to confirm a product's provenance. Research into objective measures for supply-chain assurance (e.g., cryptology-based markers) is needed to achieve these aims.

Enforcing Security Principles

Better techniques are needed for enforcing security principles where efficacy and efficiency are lacking in current mechanisms. Several important system requirements are noted below:

Authenticate users, devices, and systems. User authentication is a traditional building block for enforcement of security policy, but deployment of strong multifactor authentication systems continues to present challenges. The proliferation of Internet of Things (IoT) and autonomous systems increases the need for strong and efficient authentication of devices.

Control access. Access controls build upon authentication to support the implementation of security policies and authorizations. Systems often rely on coarse-grained access controls even though more robust mechanisms such as role-based access controls are available. To accurately enforce security policies, improvements in access control efficiency are needed for system administrators.

Use encryption mechanisms to protect data. When standard protection mechanisms fail and an adversary gains access to an IT system, or when data are transmitted across networks where eavesdropping is possible, cryptographic methods could deny intruder access to plaintext data and ensure that adversary modifications do not escape notice. Decryption of data is currently required to perform system operations or modifications, thus creating opportunities for a patient adversary; more efficient techniques that operate directly on encrypted data would offer greater security and privacy. Cryptographic tools and techniques are also needed for constrained environments (e.g., lightweight cryptography) and for long-term confidentiality (e.g., quantum-resistant cryptography).

Mitigate vulnerabilities. Current systems continue to include many legacy components with undiscovered and unmitigated vulnerabilities. Technologies are needed to neutralize malicious cyber activities on legacy systems. Data analytics offers new opportunities to capitalize on security data and identify malicious activities in the absence of established signatures. However, as discussed later in the AI and Privacy Priority Area sections of this Plan, data analytic strategies can raise new security and privacy challenges of their own, such as adversarial machine learning and leakage of private data.

Detect

Detection seeks to ensure that system and network owners and users have situational awareness and understanding of ongoing (authorized and malicious) activities and move towards largely automated detection and warning abilities.

Challenges

Provide situational awareness. Systems and networks are highly complex, and device mobility increases complexity. To defend networks and systems, it is necessary to identify all of a system's critical assets, when devices have been added or removed, and attributes and anomalies associated with the users. Real-time change detection is essential, including schemes that are flexible for dynamic network conditions and enable comparisons against known good system states.

Detect vulnerabilities. Changes in system configuration, installation of new applications, or discovery of new techniques may reduce a system's level of protection or create new vulnerabilities. Tools are required to identify shortcomings in protection measures in near real-time so the situation can be remediated. Qualified personnel to serve on vulnerability assessment "red teams" are scarce.

Effectively detect rapidly evolving malicious cyber activities. Operations are highly dynamic, and context is significant; as a result, current tools have many false positives and false negatives and fail to differentiate malicious cyber activities from authorized operations. Many techniques for recognition of malicious cyber activities are also retrospective in nature: these tools look for malicious activities that conform to a known historical pattern. Such tools are rendered useless when faced with innovation by an adversary. R&D is required to ensure that detection techniques can reliably detect the full range of adversaries' malicious cyber activities and reduce detection time. In particular, tools are needed that can detect zero-day malware and innovative sequences of operations with acceptable levels of false positives and negatives. Behavioral intrusion detection and heuristic tools, which look for anomalies compared to system baseline activities, offer a promising avenue of research. Scalable mathematical techniques capable of extracting useful information from extremely large datasets could lead to more effective detection of malicious cyber activities from data sources such as network logs.

Respond

Effective defense entails the ability to adapt, counter, recover, and adjust to malicious cyber activities. Cyber defenders must respond rapidly and effectively to adversarial activities whether precisely targeted or on a global scale. Systems must withstand these events such that their critical mission and operational functions still meet minimum performance requirements and substantial damage is avoided. Resilient systems will continue to perform correctly during and after such activities and will recover from adverse effects. To sustain resiliency, systems must also dynamically adapt to changing threats. Moreover, effective response includes countering malicious cyber activities by imposing additional costs on adversaries. Countering is aimed at exposing, degrading, disrupting, or blocking malicious activities.

Challenges

As cybersecurity technologies are integrated into complex systems and systems of systems, responses often have unforeseen dependencies and coupled interactions. Developers and users need visibility and insight into these system behaviors, as well as analytic techniques and response pathways that maintain clarity and trust and avoid unintended consequences.

Another challenge comes from the increasing use of autonomous systems, which must support response, recovery, and adjustment with little or no interaction with (or even knowledge on the part of) cyber defenders. The implications of autonomy must be considered as resilience design principles and technologies advance.

Multiscale risk governance presents technical challenges to current cyber defense activities. Decisions that increase, decrease, or shift factors that contribute to risk are made at many levels and at multiple scales. Decisions made at one level can affect other levels in complex and difficult-to-understand ways. Technical approaches are needed to identify and understand risk dependencies and explore resulting decision spaces. Complicating this process is that the time within which decisions must be made and implemented continues to shrink: detection, assessment, and mitigation of cyber threats and malicious activities must occur faster than the speed at which adversaries can exploit systems. In this evertightening risk management cycle, information sharing and coordination among decision makers becomes increasingly crucial.

Therefore, to improve the overall ability of systems to respond, R&D activities should improve the capacity of systems, enterprises, and critical infrastructure to adapt, counter, recover, and adjust in the three ways described below:

Provide dynamic assessment. Measure key properties and attributes of system components and assess potential damage amidst evolving threat methodologies and system requirements, thereby enabling response and recovery to a known good state.

Include adaptive response. Provide methods to adjust to actual, emerging, and anticipated disruptions, so that mission and organizational needs can continue to be met while unintended consequences and adversary returns-on-investment are minimized. These methods will support risk trade-offs in homogeneous enterprise systems in the near term and in integrated heterogeneous cyber-physical systems in the medium term. In the long term, they will enable integrated resilient architectures that are optimized for the ability to absorb shocks and speed recovery to a known secure operable state. R&D is needed to prevent adversaries from exploiting autonomous functions and the machine learning that underlies them.

Coordinate at multiple scales. Provide methods to manage risks at multiple scales (e.g., component, device, system, systems of systems, enterprise, or international coalition) and enable comprehensive and collective responses to specific types of malicious cyber activities, such as distributed denial-of-service attacks. These methods support the collection of threat intelligence in the near term, coordination of defensive activities in the medium term, and negotiation and orchestration of collective defenses in the long term.

Priority Areas

To advance the objectives of the Administration's 2018 *National Cyber Strategy* and FY 2021 Research and Development Budget Priorities Memorandum and tackle emerging or existing cybersecurity challenges that require coordinated, multiagency research efforts, this Plan identifies six areas for priority R&D. These Federal cybersecurity R&D priorities are not the exclusive domains where R&D is needed; additional cybersecurity R&D is needed for capabilities important to specific agencies or government missions. Advances in the priority areas will also strengthen cybersecurity across all four defensive capabilities, as illustrated in Table 1.

Table 1. Priority areas and their impact on cybersecurity

		Defensive Elements			
		Deter	Protect	Detect	Respond
Priority Areas	Artificial Intelligence	✓	✓	✓	✓
	Quantum Information Science		✓		
	Trustworthy Distributed Digital Infrastructure		✓	✓	✓
	Privacy		✓		
	Secure Hardware and Software		✓	✓	
	Education and Workforce Development	✓	✓	✓	✓

Artificial Intelligence

Artificial intelligence enables computers and other automated systems to perform tasks that have historically required human cognition and what are typically considered human decision-making abilities, as noted in the *National Artificial Intelligence Research and Development Strategic Plan: 2019 Update*.[9] In view of the substantial growth in interest and investment worldwide in applications of AI technologies, the 2017 *National Security Strategy of the United States of America*[10] calls for increased R&D investment in AI. In February 2019, the President issued an Executive Order on Maintaining American Leadership in Artificial Intelligence whose objectives include advancing AI R&D as a national objective, preserving privacy, protecting confidentiality, maintaining safety and security, developing AI technical standards to minimize cyberattacks, and cultivating public trust in AI technologies.[11] In support of the Executive Order, the *National Artificial Intelligence Research and Development Strategic Plan: 2019 Update* defines the priority areas for Federal investments in AI R&D.

AI has significant potential impacts on national economy and security; it is thus essential to guard AI technologies from unintended uses and hostile exploitations by leveraging cybersecurity practices. The emerging threats posed by AI-enhanced autonomous systems deserve serious attention. Conversely, AI techniques are expected to enhance cybersecurity by either automating certain routine tasks or assisting human system managers to monitor, analyze, and respond to adversarial threats to cyber systems. This Plan highlights the mutual needs and benefits of AI and cybersecurity.

[9] https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf

[10] https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[11] https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

Challenges

AI systems design should be informed by security, safety, and privacy principles. While these principles are not synonymous and in fact can be in tension, there are common characteristics upon which converged results can be achieved: reproducibility, accountability, interpretability, explainability, verifiability, transparency, and reliability. Existing cybersecurity concepts may have to be reformulated and redesigned to cope with AI models, algorithms, and the human-AI system interactions. Below are key issues at the interface of AI and cybersecurity:

- **AI effects on operational speed and scale.** AI systems operate at speeds and scale beyond human and current technological capabilities. This is of concern in areas where malicious activities may be driven by AI, leading to an increasingly asymmetric engagement between attackers and defenders unless AI is likewise used for cyber defenses. In general, AI systems will enable more sophisticated and automated cyber defense, and if not implemented with appropriate controls, could also be wielded offensively to perform malicious activities.
- **Interpretability, explainability, and transparency of AI.** Reasoning used in AI systems is very different from that used by humans and is not always intuitive to humans. Even though some individual algorithms used in AI can be comprehensible, their collective behavior may not always be. Thus, being able to understand, interpret, explain, and anticipate AI outputs and outcomes with transparency is difficult. Assessing biases in data or AI algorithms and guarding against these potential biases without compromising privacy will contribute to creating trustworthy AI, as will strengthening AI's accuracy, resiliency, safety, reliability, objectivity, and security. This raises questions such as how to model and measure trust in AI systems, and what levels of certainty should guide deployment of these types of systems. This is of concern in cybersecurity areas such as situational awareness, threat and risk estimation and management, privacy risk mitigation, and resource allocation.
- **Vulnerability of systems with AI components.** Many machine learning (ML) algorithms are subject to attacks throughout their lifecycles. The following kinds of attacks can take place at any stage: poisoning datasets to degrade model quality, creating backdoors that allow model creators access to other systems, crafting instances that induce classification errors, and inference attacks on both the model itself and on the dataset used to train it. Although the vulnerability surface of AI/ML is not yet well understood, it must be accounted for in AI/ML implementations. In this respect, the threat models for AI systems differ from traditional software- and/or hardware-related threats.
- **Efficacy evaluation of AI cybersecurity systems.** AI is increasingly becoming part of technologies that are central to our daily lives, such as healthcare and transportation. The boundaries between the cyber, the physical, the social, and the economic are ever more blurred. While this results in efficiency gains, it also increases dependencies and increases exposures to natural, manmade, and programmatic accidents and threats. This raises the likelihood of systemic risks and cascading harms from threats in one domain spilling over into other domains. AI introduces more complexity on top of existing, insufficient understanding of the efficacy of current cybersecurity technologies, such as how much security can be gained from investing in certain controls, and which controls best reduce risk. Measuring the multidimensional causal links between AI-based security controls, levels of resulting security, and outcomes in the face of threats is a significant challenge.

R&D Goals

- Simulate different decision-support scenarios with respect to threat models, including attacker/defender strategies related to specific AI/ML implementations, to avoid endless attack-defense cycles perpetuated by AI/ML techniques. Expand and explore new AI-based techniques for cybersecurity tasks beyond malware and intrusion detection and beyond signature-based approaches. Develop automated orchestration of security capabilities that use AI.

- Study the behaviors of AI systems, including their behaviors in the presence of human interactions, in order to make the systems trustworthy. Develop methodologies to validate and interpret results from AI systems against human perceptions and expectations. Develop techniques to improve provenance of results produced by AI systems.
- Develop tools and techniques for understanding attacks and defenses against ML systems. Improve formal method techniques to verify security and robustness of ML algorithms at both training and deployment times. Find cryptographic methods to ensure tamper-resilient storage of training data and tamper-resilient computation for ML, and to enable data sharing for machine learning without disclosing the sources or sensitive information. Develop new AI-based capabilities that can accommodate semantic security properties. Study potential vulnerabilities of chips, processors, and special-purpose devices built for AI applications, in view of the emergence of AI and neuromorphic chips and processors that feature in-memory processing and analog computing.
- Develop models, definitions, and metrics of security and trust that can be used to evaluate AI cybersecurity systems and AI-based cybersecurity controls. Ensure that security, safety, and privacy be preserved at different levels of abstraction, from high-level planning and decision-making to low-level execution of AI systems.

Quantum Information Science

Quantum computing raises the possibility of some current data encryption systems being defeated. For this reason, the Administration's 2018 *National Cyber Strategy* points out the potential impacts of quantum computers. Recent progress in realizing small-scale quantum computers demonstrates the commercial and public interest in these devices. While there is a vast gulf between these devices and large-scale quantum machines that would threaten current cryptological standards,[12,13] the anticipated impacts on security necessitate early planning to ensure that the national cybersecurity goals are met.

In addition to quantum computing, other key quantum technologies identified in the Administration's September 2018 *National Strategic Overview for Quantum Information Science*[14] include sensing; position, navigation, and timing; and communication. Together with quantum computing, these applications are poised to shape future directions for QIS and cybersecurity research. There are two questions to consider at the interface between the two fields. The first question is whether or how quantum technologies can impact or break current cybersecurity methods; hence, securing communications and computation becomes vital. In fact, the *National Defense Authorization Act for Fiscal Year 2019*[15] cited "secure communications and cryptography" in its call for a quantum information science and technology R&D plan. The second question is how to protect future quantum computing infrastructure and quantum information technology from attacks. Since quantum

[12] National Academies of Sciences, Engineering, and Medicine. *Quantum Computing: Progress and Prospects*. Washington, DC: The National Academies Press (2019); https://doi.org/10.17226/25196.

[13] National Institute of Standards and Technology. "Post-Quantum Cryptography," last updated October 22, 2019; https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline.

[14] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf

[15] https://www.congress.gov/bill/115th-congress/house-bill/5515/text (Section 234).

technologies are fundamentally different from their conventional counterparts, it is imperative to address potential security flaws as the devices and systems are designed.

Challenges

Future quantum technologies should be secure by design, from hardware to software and including the protocols that link quantum systems. Since debugging errors in quantum software and hardware is highly nontrivial due to quantum mechanical effects, correct-by-construction implementation is desirable. Conversely, because quantum technologies hold promise for achieving a higher level of security beyond classical computing limits, understanding quantum capabilities and finding ways to circumvent their fundamental limits have far-reaching implications. Below are the overarching challenges:

- **Securing quantum software.** Trusted and assured software stacks for controlling quantum computers, processors, and devices are critical because, unlike the conventional software testing process, the states of quantum programs cannot be directly examined for potential errors. Quantum programs that operate directly on a quantum device should utilize the laws of quantum mechanics to prevent illegal operations. Computational effects of quantum programs are presently unknown.
- **Securing quantum hardware.** Testing and debugging hardware components are difficult tasks due to quantum mechanical effects. Current knowledge of side-channel attacks on quantum devices is confined to quantum key distribution (QKD). A broader look at the issue of general quantum hardware is desirable. Moreover, as quantum systems will likely be built from different types of quantum hardware platforms, the resulting heterogeneous platforms and their interconnects are likely to be targets of attacks.
- **Designing efficient quantum cryptographic protocols.** Efficient protocols (beyond QKD) are still elusive for designing quantum information, communication, and computation with security requirements stronger than classical settings, and systems must be robust to noise and feasible to implement. Composability of quantum and/or classical resources is not well understood. Classical proof techniques for establishing security of protocols do not always carry over to the quantum settings.
- **Anticipating quantum attacks and countermeasures.** Known methods of attack perpetrated by quantum technologies on current systems are relatively few, e.g., Shor's algorithm and attacks on QKD systems. Countermeasures against quantum attacks are also scarce, e.g., device-independent quantum information.

R&D Goals

- Design type-safe quantum programming languages for controlling quantum processors and for interacting with quantum memories. Understand the side effects of programming a quantum computer, especially in the presence of quantum effects and noise. Design and build tools to analyze quantum programs akin to formal method techniques for classical software and protocols.
- Explore new theoretical and experimental methods to probe quantum states, quantum processes, and their quantum properties to diagnose and analyze hardware for its security properties. Find algorithms and experimental techniques to efficiently test and evaluate quantum hardware or devices for functional correctness.
- Draft standards for quantum-resistant cryptography while observing the recommendations of NIST and the National Security Agency. Devise a plan for implementing quantum-resistant cryptography while studying its potential vulnerabilities. Integrate classical, quantum-resistant, and quantum cryptographic techniques. Design, analyze, and test quantum security protocols,

beyond QKD, for security and efficiency. Extend these protocols to multiparty scenarios whenever possible. Demonstrate a small number of protocols to validate their utility on quantum systems.

- Understand how quantum technologies can be exploited for attacks on classical and/or quantum systems. Understand security threats against quantum devices and their supply chain, including materials designed for various physical platforms. Design security models, craft provably secure countermeasures against quantum attacks, and demonstrate the feasibility of these defense mechanisms.

Trustworthy Distributed Digital Infrastructure

A trustworthy distributed digital infrastructure (TDDI) is a critical enabling element for the United States to underpin the growth of new industries that will help drive the Nation's economic growth and keep the Nation as the world leader in innovation. This imperative is recognized in the Administration's 2018 *National Cyber Strategy*, specifically to "facilitate the accelerated development and rollout of next-generation telecommunications and information communications infrastructure in the United States,"[16] which includes the deployment of advanced fifth-generation (5G)-and-beyond wireless networks.

A TDDI will help distribute computing to the new network edge, enabling a wide range of applications and societal benefits for manufacturing, healthcare, smart grids, autonomous vehicles and mobility, and smart cities. Recognizing this opportunity, the Administration's FY 2021 Research and Development Budget Priorities Memorandum calls for agencies to prioritize R&D to "lower barriers to the deployment of surface, air, and maritime autonomous vehicles."[17]

Challenges

5G and Post-5G Wireless Security and Resiliency

5G wireless networks are poised to transform the world's digital infrastructure, supporting a connected society with higher data rates, lower latency, and higher reliability. While the underlying technologies for 5G are largely complete, research is needed into cost-effective means to ensure secure and resilient communications over potentially untrusted infrastructure. A significant area of concern is securing the information and communications technology and services supply chain underlying 5G technology.[18]

Additionally, research is needed to shape the capabilities required in the next generation of networking technology, including faster, higher-bandwidth 5G and post-5G networks, and secure autonomous spectrum sharing.[19] It is critical to design security from the beginning into all layers of post-5G networks and services, from mobile devices through radio access and core networks, to the Internet, and into enterprise systems and applications.

Edge and Fog Computing

Cloud computing continues to grow year after year, particularly in the infrastructure-as-a-service sector. Increasingly, cloud applications need to provide feedback to end users in real time. The low-

[16] 2018 *National Cyber Strategy*, p. 15.

[17] Memorandum M-19-25, p. 4.

[18] "Executive Order on Securing the Information and Communications Technology and Services Supply Chain" (May 15, 2019); https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[19] Executive Office of the President. *Research and Development Priorities for American Leadership in Wireless Communications* (May 2019); https://www.whitehouse.gov/wp-content/uploads/2019/05/Research-and-Development-Priorities-for-American-Leadership-in-Wireless-Communications-Report-May-2019.pdf.

latency requirements are pushing analytics and data processing close to the network edge where the data are first collected. Fog and edge computing have emerged to meet this need.

In fog computing, computation and storage are moved as needed to nodes between cloud servers and edge nodes. Computations that require only local data can be performed at the intermediate nodes, while global processing continues to be performed in cloud servers. This hierarchy of data processing services has evolved to become a new paradigm, with fog nodes communicating directly with each other as needed to perform global-level computations.

Edge computing started as the introduction of applications in mobile network base stations, but it has developed into an edge-centric computing paradigm in which edge nodes communicate in peer-to-peer fashion to perform tasks and compute data of immediate local value. This computing paradigm can take advantage of fog and cloud nodes to provide stable resources when needed.

End-to-end security becomes complex and challenging when data are located in centralized cloud servers, intermediate fog nodes, and edge devices. Addressing this context, the 2019 *Federal Cloud Computing Strategy*[20] recommends implementing security controls at the data layer in addition to the network and physical layers, thus providing a multi-layer protection strategy.

Internet of Things

The Internet of Things is now a reality as a growing number and variety of consumer devices, home appliances, and sensors used for transportation and municipal services share compute power, network connectivity, and ability to be controlled remotely. The IoT environment is complex, and its security challenges are just as complex. IoT devices are often limited in computational, data storage, communication, and available power resources. Approaches to authentication, encryption, and security policy enforcement that work for the desktop and server environment will not be deployable to a resource-constrained device. Usability and human factors are also a challenge for the secure design of IoT because the devices have limited user interfaces, and the typical user of consumer devices is not trained in cybersecurity and may not make reliably good security and privacy decisions.

Cyber-Physical Systems and Critical Infrastructure

Cyber-physical systems (CPS) are engineered systems that are built for and depend upon the seamless integration of computation and physical components. Examples of such systems can be seen in "smart," Internet-connected manufacturing assemblies, traffic flow controls, rescue robots, border security drones, and consumer medical devices, among a host of others. Advances in CPS will enable advanced capability, adaptability, scalability, resiliency, safety, security, and usability that will expand the horizons of these increasingly critical systems.

As CPS systems become more complex, the interdependence of components increases the vulnerability to attacks and cascading failures. The algorithms that control CPS may be complex and opaque, and their security may depend on autonomous cyber defense rather than human intervention, as well as on secure analog and digital electronic hardware. Furthermore, restoration and resiliency of CPS systems after a fault or cyber attack may be challenged by the potential overload on the physical systems.

R&D Goals

- Develop methodologies and standards to support seamless, end-to-end security across interconnected networks with multiple owners, trust domains, topologies, networking

[20] https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf

paradigms, and the full range of mobile devices and mobile network layers. Enable secure ad hoc establishment, management, and disposal of tailored trust domains within a larger general-purpose infrastructure. Develop software assurance solutions for virtualized radio access networking and for security of software-defined networking for the core network. Design analog and mixed-signal solutions at the wireless end points, where radio frequency components play critical roles, to assure secure and reliable autonomous transceiver reconfiguration, antenna beamforming, and dynamic spectrum utilization.

- Develop technologies to sustain autonomous management of security across the communication infrastructure in ways that balance strength of security services with performance requirements of availability, latency, processing, and storage capacity. Develop data-centric security solutions based on the protection requirements of the data across all networking paradigms: cloud, fog, and edge computing. Devise privacy protection mechanisms that can be tailored to the location and role of a node in a combined sensing/communication/computing paradigm—from the sensor where raw data lack context, to more robust protections as the aggregation of data increases in volume and source diversity.
- Develop end-to-end security and key management capabilities that will allow highly secure, highly resourced nodes to interoperate with resource-limited edge and IoT devices. This includes devising effective access control, authentication, cryptography, and key management techniques for limited-resource nodes. Develop technologies to attest and verify devices and systems at varying levels of computational capabilities.
- As CPS systems (e.g., cars, medical devices, and utilities) scale in the number of devices they connect and the volume of data they process, develop approaches to assure that they remain resilient to adverse cyber activities. This includes developing accurate models of CPS environments to reduce vulnerabilities and mitigate the impacts of incidents and failures. Develop methods and technologies that will successfully integrate human decision-making with cybersecurity technologies and process control technologies. Advance formal methods to validate high-assurance, fault-tolerant, adaptive subsystems that can operate in contested and degraded conditions for long periods without human interaction.

Privacy

Privacy is a confluence of multiple values such as solitude, confidentiality, and autonomy that define an individual's control of personal information, identity, or the boundaries of personal spaces. Privacy comprises a multitude of disciplines: ethics and philosophy, sociology and psychology, law and government, economics, and technology. Broad recommendations for R&D in privacy have been presented in the 2016 *National Privacy Research Strategy*.[21]

In the context of cybersecurity R&D, this Plan focuses primarily on privacy aspects that involve collection, disclosure, and use of an individual's private information, including identity; patterns of behavior; and economic, social, or other discriminators. Confidentiality and integrity principles necessitate controls that limit unauthorized access, use, and disclosure of data. Security can be the mechanism by which privacy risk is prevented, reduced, or mitigated when the data or system to be secured implicates privacy interests and values. However, secure systems might be in tension with privacy, especially when considering the security principle of availability. This is manifested when users' desires to control privacy-relevant data run up against the needs of system stakeholders to control that same data for authorization, attribution, and/or monitoring for situational awareness,

[21] https://www.nitrd.gov/PUBS/NationalPrivacyResearchStrategy.pdf

decision support, risk modeling, incident response, and/or threat scoring. Nevertheless, cybersecurity research must consider privacy management as a fundamental aspect of the design of secure systems.

The following challenges need to be overcome to ensure that individuals' privacy is protected in an open, highly digitized economy, and to ensure that U.S. Government agencies, commercial entities, and social networks can access and use personal data in authorized ways without putting individuals' personal privacy at risk.

Challenges

- **The difficulty of designing privacy-protecting systems.** People value privacy differently, perceive privacy-related harms differently, and vary their privacy requirements with circumstances. To develop systems that are more respectful of peoples' privacy choices, system designers and developers need to better understand what people value regarding privacy, what people's privacy desires and expectations are, and the ways privacy might be infringed upon.
- **The lack of appropriate tools for designing systems.** System designers need tools that incorporate effective privacy requirements and controls. Even when designers do consider privacy at the beginning of the design process, they lack a systematic approach for understanding and assessing the risks that a system might pose to privacy, for identifying and expressing privacy requirements for a system, and for designing controls that can achieve those goals.
- I**ndividuals' needs not only to understand the rules that govern the use of personal data, but also to have confidence that the rules are observed in practice.** Techniques are needed that will facilitate people's expression and implementation of privacy preferences. Furthermore, advances are needed in technologies that can assure that personal data are linked with the rules appropriate for the context in which they are collected and that operations applied to those data are governed by those rules.
- **Privacy concerns deriving from the growing interest in publishing statistics, analyses, and raw data that involves people**. Existing approaches for protecting privacy, such as the removal of personally identifiable information, have not been able to address the privacy risks of large-scale data collection, analytics, and release. As more information about individuals is stored and made available, data analytics can often be used to link sensitive information back to individuals, despite efforts to anonymize the data. Techniques are needed to measure and balance reidentification risks against the benefits of data use and storage.
- **Requirements for effective solutions for recovery from privacy violations**. Existing recovery mechanisms are limited and are inconsistent in their efficacy. New approaches for recovering from privacy violations need to be developed that are fast, predictable, and easy to implement.

R&D Goals

- Develop research methods that can reliably and validly sample, measure, and represent people's privacy desires, expectations, attitudes, beliefs, and interests. Develop methods and technologies that can identify privacy violations and privacy harms effectively and efficiently, with the capability to assess privacy harms.
- Devise frameworks that integrate safety, security, and privacy requirements, allowing system designers and developers to reason across all three domains concurrently. Develop privacy trust models that encompass a broad range of authorized data disseminations and uses. Develop languages and reasoners to formally specify, compose, and enforce targeted privacy requirements, including translation from natural-language privacy statements or information-sharing agreements. Advance system design tools for managing privacy risk, i.e., standardized frameworks, libraries, and interfaces; tools to verify designs against privacy requirements; and

tools to standardize privacy requirements from data owners and custodians. Such design tools should support end-to-end composable mechanisms that protect the privacy of sensitive inputs at rest and in use, resulting in outputs that are tagged for privacy policy enforcement by their consumers.

- Develop efficient, robust, and agile privacy controls for distributed analytic applications that can be tailored to the privacy requirements and the available resources of each party (e.g., secure, multiparty computations). Techniques are also needed to automatically invoke and verify privacy controls in accordance with policies. Devise methods that allow composition of privacy rules of an aggregate or function output from the privacy requirements of each record or function input.
- Foster techniques and models that can systematically assess and quantify privacy risks, such as the effectiveness of privacy protections and changes in privacy risk when disclosed personal information is correlated with other information. Develop metrics and measures of reidentification risk for disclosed and obfuscated data, both at the time of disclosure and obfuscation and over subsequent accesses, uses, and potential correlations with other data.
- Develop models, techniques, and evaluation metrics for redress and recovery from privacy violations, such as provable assurance that personal information is removed from a dataset or is otherwise rendered inaccessible. Research techniques to identify and redress inaccurate or unauthorized personal information informing machine learning models.

Secure Hardware and Software

Computing today is geospatially dispersed—ranging from mobile edge devices to data centers—and highly heterogeneous in nature—ranging in capabilities from tiny microcontrollers, mainstream CPU, GPU (graphics processing unit), and reconfigurable processors to highly customized NPUs (neural processing units). Computing systems execute highly diverse tasks ranging from sensing, perception, planning, and data processing to complex scientific applications where computation and data may be offloaded from one system to another continuously for performance, load-balancing, and fault tolerance. Data and storage are geo-replicated, and the network evolves with time. Vulnerabilities and defects of any remotely accessible software can have significant cybersecurity consequences for the system. Software is developed with vulnerability and defect rates that force dependency on a detect-and-patch paradigm that is expensive and ineffective. Against this backdrop, securing data, codes, and computation from hardware and software to network and storage poses significant challenges. The tools and capabilities of adversaries improve with time. Assumptions about threats need to be reevaluated and defenses need to be adapted constantly.

The foundation of security is authentication of hardware, attestation of low-defect software, and secure software updates to migrate a system forward by revoking compromised assets and patching newly discovered vulnerabilities. Secure root-of-trust provides such a foundation for these functions by establishing an unforgeable identity that remains inseparable from the computing assets and provides a small trusted computing base with hardware-protected cryptographic keys used for these purposes.

Secure hardware and software are a required foundation for the modernizing of U.S. military forces, as identified in the 2018 *National Defense Strategy of the United States of America*.[22] This foundation enables the development of resilient and survivable cyber capabilities, federated networks and information ecosystems, missile defenses, nuclear forces, autonomous systems, and other critical functions

[22] An unclassified summary of this document is available at https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

identified in the *National Defense Strategy*. The development of a secure hardware and software foundation are further supported in the 2018 *National Cyber Strategy*.

Challenges

The following paragraphs describe cybersecurity challenges in hardware (HW) and/or software (SW), as indicated in the side headings:

- **Trusted hardware and secure supply chain (HW)**. The foundation of computing is built on the premise that hardware can be trusted: the hardware executes as specified and does nothing less and, more importantly, does nothing more, i.e., it does not execute instructions or functions without explicit commands to do so. Since much hardware originates offshore, maintaining trust in the hardware supply chain is crucial. Hardware Trojans or backdoors that exfiltrate information remain a great concern. Other concerns relate to theft of intellectual property; compromised supply chain with aged or untrusted parts; and verification of third-party intellectual property, which may be cloaked with unknown features that increase the attack surface or add complexity that makes verification difficult.
- **Adverse possession (HW/SW)**. In a distributed computing environment, there are multiple opportunities for an adversary to gain physical possession of a remote device, allowing the adversary to observe the device functions, obtain data/memory/software dump, de-package and reverse-engineer hardware, supply malicious inputs to the system, and emulate device behavior. Both a remote device's hardware and software must stand up to physical attacks.
- **Hardware vulnerabilities (HW).** It is difficult to patch hardware vulnerabilities. Recent attacks against commercial microprocessors demonstrate the vulnerabilities of microprocessor systems.[23]
- **Design-for-security (HW/SW).** Both hardware and software should be designed with security considerations right from the beginning of the design process. Security features such as authentication, access control, and encryption are relatively well understood, yet design-for-security has remained elusive due to lack of good security abstractions, lack of integrated tool suites to aid in secure design, and the economics of design. There is a need for quantifiable and measurable security abstractions that effectively capture current and future attacks to advance design-for-security, short of which, defensive design will remain a piecemeal approach prone to vulnerabilities. Similarly, there is a need to define roles and permissible actions for various actors, including users, system administrators, and underlying software systems, early in the design cycle to formally verify the security of systems against these roles.
- **Economics of security (HW/SW).** Economics of design favors component reuse, often resulting in feature sets larger than necessary, which increases the attack surface and compounds verification problems. Furthermore, developers are less likely to provide the low-defect software that security requires if doing so imposes time and effort penalties.
- **Secure update (SW).** It is crucial that the software of a system remains updatable to allow newly learned vulnerabilities to be patched, compromised assets to be isolated and contained, and software to evolve as needed.
- **Effective management (SW).** Software systems must be designed so the security and privacy aspects can be effectively configured and managed, and so they take into consideration the various levels of expertise of the people charged with performing such tasks. Security for software

[23] National Academies of Sciences, Engineering, and Medicine. *Beyond Spectre: Confronting New Technical and Policy Challenges: Proceedings of a Workshop*. Washington, DC: The National Academies Press (2019); https://doi.org/10.17226/25418.

systems also must address their continual evolution through development and operational phases as defects are detected and fixed; new missions, markets, and platforms are targeted; and new capabilities are added. Further, fixing software defects imposes a risk of introducing additional defects, which squarely points to a need for improved management of software development and testing.

R&D Goals

- Develop cost- and threat-proportionate integrated root-of-trust alternatives for various hardware devices, ranging from low-cost IoT devices and networked sensor devices to server computers. Develop techniques for authenticated secure boot, authenticated secure software updates, and authenticated secure software execution with security guarantees extending from the hardware layer to the application layer.
- Develop novel processes, techniques, and mechanisms that protect against reverse-engineering efforts.
- Develop mechanisms and tools that verify the security properties of hardware.
- Develop secure debug and testing techniques. Develop crypto-agility to migrate existing advanced encryption standards-based infrastructure to post-quantum cryptographic solutions. Develop hybrid cryptography schemes for cost-proportionate security. Develop efficient general solutions against code-reuse attacks.
- Develop new software development methodologies that allow rapid revision and regression against security goals.
- Develop secure update mechanisms that support the full range of product formats (i.e., proprietary and open source); applications (e.g., enterprise services and IoT); and lifecycles.
- Develop empirical understanding of software defect rates, effort, and calendar time that are achievable with alternative software development and sustainment technologies, and of relationships between software defects and software vulnerabilities. Based upon empirical understanding, develop paradigm and supporting technology to develop and sustain software with less than 1 defect per 100,000 lines of code (LOC) without compromising quality attributes, cost, or schedule. Develop tools and techniques for effective management of software systems.

Education and Workforce Development

There is a shortage in the United States of qualified cybersecurity workers, and the supply-demand gap is increasing in both quality (the competence required) and quantity. This gap threatens all sectors of the national critical infrastructure and will throttle aspirations in the advancement of AI and QIS. The gap is deeply rooted in the education and training infrastructure; it includes a shortage of qualified teachers, trainers, and advanced faculty.[24]

The current culture of treating cybersecurity as an add-on requirement is a barrier to effective, efficient solutions and complicates the successful adoption of innovative technologies. The sociotechnical challenges involving human, social, organizational, economic, and technical factors, and the complex interaction among them require engagement with all sectors of society. This requires increasing diversity and inclusion and broadening participation in the R&D community. In addition, scientists and engineers often lack experience in business formation and may not understand the commercial viability of their innovations, hindering the effective transfer of technology to products.

[24] https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf

Challenges

Cybersecurity education and workforce development, as emphasized in the 2018 Federal STEM Education 5-year plan, *Charting a Course for Success: America's Strategy for STEM Education*,[25] form a critical element for successful implementation and transition to practice of any advances in cybersecurity R&D. The Nation needs to make cyberspace worthy of the public's trust by investing in an education and training ecosystem that supports the application of "systems security engineering"[26] capabilities at all proficiency levels. Challenges in developing the requisite education infrastructure include the following:

- **Emphasizing education imperatives in two broad categories**: (1) professional careers in cybersecurity related science and technology, and (2) the general population of users of safe and secure cybersecurity infrastructure.
- **Expanding student and worker support, with a focus on broadening participating by underrepresented groups,** via scholarships, fellowships, and educational grants; internships, apprenticeships, and cooperative learning opportunities; consortia-based structures for education, with job rotation and cross-pollination between government, industry, and academia; and incentives for early and sustained mentoring, especially for traditionally underrepresented populations.
- **Supporting innovative K–12 and after-school curricula** to introduce technological awareness topics, expand adoption of transformative technological breakthroughs, and engage K–12 students and teachers to increase student interest in cybersecurity careers.
- **Increasing the capacity of the U.S. education enterprise** to produce cybersecurity professionals and expanding adaptability in critical areas such as the secure use of AI, quantum computing, advanced manufacturing, and emerging wireless technologies. This includes continuous reskilling of the workforce in order to keep up with the rapidly evolving IT technologies and providing funding to the academic research community—for both pure and applied research—to create and expand cybersecurity programs aligned to near-term development of enabling fields identified in this plan.
- **Expanding postsecondary cybersecurity faculty** by offering fellowships, retraining existing faculty, and preparing nonacademic researchers to become faculty.
- **Preparing future scientists and engineers to extend their focus** beyond the university laboratory to accelerate the economic and societal benefits of research projects that are ready to move toward commercialization by building a more entrepreneurial R&D workforce to support innovation and use the advancements described in the other priority areas of this Plan. This includes identifying grand challenges to foster innovation among faculty and students and to promote multistakeholder coordination and linkages; such challenges may include emergence of hypertransformative technologies that may necessitate changes in learning processes or a large realignment of education with newly identified needs of the future workforce.

R&D Goals

- Accelerate adoption of a modern taxonomy of the cybersecurity workforce, such as the *National Initiative for Cybersecurity Education—Cybersecurity Workforce Framework*.[27] Conduct research on effective models to educate individuals of different backgrounds and ages to protect themselves from cyber threats and inappropriate content on the Internet.

[25] https://www.whitehouse.gov/wp-content/uploads/2018/12/STEM-Education-Strategic-Plan-2018.pdf

[26] https://doi.org/10.6028/NIST.SP.800-160v1

[27] https://doi.org/10.6028/NIST.SP.800-181

- Research innovative ways to develop talent in all sectors of society to build the cybersecurity workforce, improve the preparation, increase the participation, and ensure the contributions of individuals from groups that have traditionally been underrepresented and underserved in science and engineering. Study effective models and ecosystems used in other countries to understand how to build partnerships in support of developing cybersecurity talent.
- Study the supply-and-demand forces in the innovation workplace to help predict future workforce needs. Include considerations of educational pathways and potential retraining opportunities.
- Support experiential learning, such as apprenticeships, internships, job-shadows, and other employer-educator partnerships, to align curriculum with workplace demands. Apply the research to develop systems that enable reskilling Americans for the jobs of today and the future. Promote distributed, highly scalable educational tools and expand the use of mentoring and apprenticeship as force multipliers in critical areas. Engage in strategic cybersecurity educational planning that considers how emerging technologies—including artificial intelligence, machine learning, and quantum information sciences—alter the cybersecurity focus of the Nation's workforce.
- Accelerate adoption of convergence research among faculty and students to solve complex scientific, engineering, and societal problems that require integrating knowledge, methods, and expertise from different disciplines and forming novel frameworks to catalyze scientific discovery and innovation.
- Focus not only on developing the expertise and talent to build these systems but also on research that addresses how the education and training ecosystem can develop interdisciplinary approaches that support innovation. Conduct research to identify cybersecurity professionals capable of fostering the technological breakthroughs most critical to developing and sustaining a safe Internet environment. Enable "use-inspired research" in government-university-industry R&D partnerships that bring pressing, real-world challenges faced by industry to university researchers; leverage industry expertise to accelerate the transition of open and published research results into viable products and services in the marketplace for economic growth; and grow research and workforce capacity by linking university faculty and students with industry representatives.

Critical Dependencies

Building on the dependencies identified in the 2016 *Federal Cybersecurity Research and Development Strategic Plan*, advancements in this Plan's defensive elements and priority areas critically depend on continuing development of the following areas (listed alphabetically).

Human Aspects

Comprehensive cybersecurity requires understanding the human facets of cyber threats and secure cyber systems, and development of an informed and skilled cybersecurity workforce and general public. Many opportunities exist in economic, human, and social research for improving cybersecurity:

- Advancing usable security research to design security techniques that improve usability and acceptability, cognitive efficiency and decision support, and collaboration both among people and with increasingly autonomous security systems.
- Conducting social and behavioral studies to help identify the strengths and weaknesses of incentive mechanisms to acquire and deploy cybersecurity measures.
- Developing psychological, sociological, and economic models of human weaknesses and strengths for use in analyzing security properties in systems and the respective roles of users, developers, operators, defenders, and adversaries.
- Validating models of adversary motives and susceptibility to deterrence actions such as denial, attribution, and retaliation.
- Preventing and detecting insider threats by designing systems, both human and technical, that can better identify insiders doing harm to their organizations' cyber systems in real time.
- Pursuing studies of organizational, social, and programmer psychology to support more effective development, deployment, and adoption of security and privacy technologies.
- Modeling social and international norms, rules of engagement, and escalation dynamics of malicious cyber activities that range from phishing and ransomware, through censorship and information campaigns, to limited- and full-scale cyber-warfare to enable identification of institutional, social, and structural factors that promote or undermine a secure cyberspace.

Research Infrastructure

Access to advanced cybersecurity testbeds continues to be a hurdle for researchers. Testbeds are essential for researchers to be able to use actual operational data to model and conduct experiments on real-world system vulnerabilities and exploitation scenarios. Current methods fall short of realistically integrating human factors into experiments and accurately quantifying them as security variables to be tested. Data repositories exist today, but many are unable to deal with proliferation of massive datasets, do not support semantically rich data searches, and have limited data provenance information. The Federal Government, with industry participation, should expand the scope and fidelity of cybersecurity testbeds in multiple application areas such as cloud computing, manufacturing, energy delivery, transportation, information and networking systems, healthcare, and telecommunications. It should also enable multidisciplinary experimentation in computer science, engineering, mathematics, modeling, human behavior, sociology, economics, epistemology, and education.

Risk Management

Technologies enable cybersecurity, but achieving appropriate levels of security requires more than technology. The application of cybersecurity technologies requires significant insight into an organization's goals, its abilities and modalities, and the nature of the threats it faces. Risk management is the ongoing process of identifying, assessing, and responding to risk. The NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*,[28] presents a generally accepted process, consistent with international standards, for information-security risk management at all levels of an organization. The NIST *Framework for Improving Critical Infrastructure Cybersecurity*[29] presents a flexible framework to help organizations manage and reduce cybersecurity risk and has been applied across a broad spectrum of organizations.

Advances in risk management, such as those below, are needed to achieve the goals of the defensive elements:

- Integrated cost modeling techniques that incorporate human factors (such as required expertise and ongoing training).
- Risk models that incorporate information about known and projected vulnerabilities.
- Integration of modeling, simulation, and exercises into risk management practice.

Scientific Foundations

Cybersecurity needs sound mathematical and technical methods with clear objectives; comprehensive theories (e.g., of defense, systems, and adversaries); principled design methodologies; models of complex and dynamic systems at multiple scales; and metrics for evaluating success or failure. Establishing scientific foundations in the areas below will directly support the goals and objectives for the cybersecurity defensive elements and priority areas:

- Formal frameworks with quantitative definitions of threats, measurable security assumptions and guarantees, and efficient formal methods for evaluating compositions of systems, defenses, and adversaries.
- Principled design techniques to construct secure systems with provable or measurable verification and validation of security properties, and characterizations of efficiency.
- Reasoning frameworks to anticipate evolving and disruptive technologies and threats.
- Theories and models aimed at understanding individual, organizational, and social needs, expectations, and behaviors around security, safety, and privacy in sociotechnical systems.

Transition to Practice

Federal agencies should increase R&D funding to cybersecurity R&D transition-to-practice activities, such as System Integrator Forums, Small Business Innovation Research activities, and consortium ventures. Streamlining and accelerating the acquisition process for the results of R&D should also remain a priority. Agencies should continue to assess and selectively utilize all contractual instruments at their disposal. For example, Other Transactions Authority can provide a mechanism to streamline and accelerate funding of R&D and allow agencies to reach performers who are typically not engaged in government-funded cybersecurity research.

[28] https://doi.org/10.6028/NIST.SP.800-39

[29] https://doi.org/10.6028/NIST.CSWP.04162018 (revised in 2018).

Implementing the Plan

Research and development funding is a scarce resource. For this reason, it is essential to invest wisely and selectively to avoid research redundancies. This section identifies the respective roles for the Federal Government, academia and research organizations, and the commercial sector; and identifies strategies for ensuring coordination of robust cybersecurity R&D among and across sectors.

Federal Research Agencies

The Federal Government is the primary source of funding for long-term, high-risk cybersecurity research initiatives. Science agencies such as the National Science Foundation have a leading role in funding cybersecurity R&D to support this Plan. Depending upon the agency, the research may be executed in-house; at national laboratories; or in academia via grants, cooperative agreements, contracts, or other agreements. The challenge for these agencies is twofold: (1) identifying and funding the most promising and important R&D initiatives, and (2) transitioning this research into practice.

Science agencies should embrace and fund multidisciplinary research and continue to demand strong scientific methods in all funded initiatives. Mission agencies, such as the Department of Homeland Security, primarily fund applied research with a near-term or mid-term horizon to meet immediate and future mission requirements. Mission-specific R&D is often incremental in nature, and agencies should make special efforts to ensure that the desired functionality is not already available from the private sector, academia, or other Federal agencies. Both science and mission agencies should avoid funding near-term R&D unless it is directly related to mission-specific needs or creates public goods that industry is not incentivized to pursue.

Research-funding agencies also have an obligation to ensure that their R&D investments promote research integrity and protect national research assets. This objective is among the priority crosscutting actions emphasized in the Administration's FY 2021 Research and Development Budget Priorities Memorandum (M-19-25). In addition, the Subcommittee on Research Security of the NSTC Joint Committee on Research Environments (JCORE) has been established to lead Federal efforts in developing guidance and best practices to ensure that the Nation's researchers are protected from undue foreign influence.[30] Agencies should coordinate their actions in this area through this Subcommittee.

Academia and Research Organizations

Academia is the leading R&D performer of basic research and long-term, high-risk initiatives. Academics are strongly encouraged to embrace this Plan's focus on measurable and testable efficacy and efficiency. Where possible, researchers should provide comparisons against open datasets to enable comparison and evaluation of competing techniques. Use of open datasets also enables reproducibility of experiments, which is a basic scientific tenet. Academic researchers should incorporate strategies for transitioning successful research into practice when developing proposals and initiating research. Academia strongly influences research directions through the promotion and tenure process. Academic institutions are strongly encouraged to value multidisciplinary cybersecurity research, even where publication occurs in nontraditional journals for the field. Institutions are also encouraged to value research with rigorously defined models and experimental design.

[30] https://www.whitehouse.gov/wp-content/uploads/2019/07/Update-from-the-NSTC-Joint-Committee-on-Research-Environments-July-2019.pdf

Research organizations and professional societies are natural partners in cybersecurity R&D efforts. They produce research strategies, organize conferences, and publish journals. By establishing publication requirements for documented efficacy and efficiency, these organizations can greatly aid and improve scientific rigor in the cybersecurity field.

Commercial Sector

Budgets for commercially funded cybersecurity research are usually comparatively modest for even the largest IT companies. Private-sector R&D funding is typically internal and focused on product-development goals based on the specific needs of the company as well as on profitability and turnaround time. While companies often have the skills to perform long-term and high-risk research, the opportunity cost of their moving personnel to address these topics is high, even when government funding is available to defray the immediate costs, because longer-term research often benefits the entire industry, not just the company that funded it. Nonetheless, there are opportunities for the R&D activities of the private and public sectors to be synergistic and complementary. A well-functioning cybersecurity research ecosystem must offer several mechanisms for the two sectors to mutually benefit each other.

Coordination and Collaboration

Coordination and collaboration across sectors are essential to avoiding redundant research initiatives. The Federal cybersecurity R&D community engages with industry via many public-private partnerships. For example, partnerships exist in the area of the trusted computing base that provides technology for hardware-based cryptography, key repositories, self-encrypting drives, and device authentication. Agencies use advisory boards to obtain industry perspectives, such as the NIST Information Security and Privacy Advisory Board.[31] Both the Department of Homeland Security and the Department of Defense have offices in Silicon Valley to expand their conversations with technology innovators. In addition, the National Cybersecurity Center of Excellence, an example of a Federal, state, and local government partnership (NIST, the State of Maryland, and Montgomery County, MD), focuses on accelerating the adoption of secure technologies.[32]

Opportunity for fruitful collaboration exists in expanding efforts to measure and verify efficacy and efficiency in cybersecurity products and services. Consumers and enterprises need such information for effective and efficient management of their cybersecurity risks. Private-sector product vendors should consider the full range of costs of using cybersecurity solutions, including financial costs, cognitive load on users, and innovation-inhibiting practices. Another fruitful partnership opportunity for commercial entities would be to jointly identify precompetitive research areas in which private-public partnership funding would be most productive.

Coordination between Federal departments and agencies is facilitated by the NSTC. Unclassified Federal R&D efforts in networking and information technology are coordinated by the NITRD Program and its National Coordination Office. Classified research efforts are coordinated by the NSTC Special Cyber Operations and Research and Engineering Subcommittee.

Federal Cybersecurity R&D Strategic Plan Implementation Roadmap

The coordinated R&D activities of this Plan are carried out by Federal agencies with varying missions but complementary roles. This arrangement assures that the full spectrum of R&D approaches is

[31] https://csrc.nist.gov/projects/ispab

[32] https://www.nccoe.nist.gov/

represented and engaged. Details of R&D carried out by each agency involved are provided by agencies through individually appropriate means, such as agency-specific strategic plans or implementation roadmaps, and via appropriate contracting methods such as solicitations or broad agency announcements.

Each year, the NITRD Program compiles and produces a Supplement to the President's Budget Request (for example, see https://www.nitrd.gov/pubs/FY2020-NITRD-Supplement.pdf) which provides highlights of agency research activities in various areas of IT and networking. In the Supplement, the section describing NITRD's Cyber Security and Information Assurance Interagency Working Group provides an overview of planned Federal investments in unclassified cybersecurity R&D. The annual *Federal Cybersecurity R&D Strategic Plan Implementation Roadmap* (an online appendix to the Supplement, available at https://www.nitrd.gov/publications/), provides information about the activities the agencies are pursuing in implementing this Plan.

Recommendations for Supporting Activities

The Federal Government can support this Plan by carrying out the following recommendations.

Prioritize basic and long-term cybersecurity research.

The Nation will benefit from a steady increase in Federal cybersecurity R&D, with an emphasis on basic research and long-term, high-risk research initiatives in the Deter, Protect, Detect, and Respond defensive capabilities. Because basic research and long-term research are areas where the private sector is not likely to invest, Federal investments will be important for R&D in these areas. Basic research should emphasize the development of sound scientific foundations and formal, reproducible, and quantifiable methods for assessing the effectiveness and efficiency of cybersecurity solutions.

Advance cybersecurity standards.

Cybersecurity standards and best practices that address security, privacy, interoperability, and usability are critical tools for reducing vulnerabilities of IT systems to malicious cyber activities. Federal agencies should continue to advance measurement science, standards, and related technologies in ways that underpin and accelerate adoption of effective, efficient, and practical security solutions and technologies. Effective cybersecurity standards will also support U.S. innovation and industrial competitiveness.

Accelerate the transition of effective cybersecurity research results into adopted technologies.

Federal agencies should streamline the technology transition process for federally funded research and develop a suite of standardized licensing or other intellectual property agreements that could be selected to facilitate technology transfer to commercial entities as well as to the Federal Government. Within its acquisition process, Federal agencies should support solutions and technologies that advance the capabilities described in this Plan. Agencies should align such efforts with the Lab-to-Market Cross-Agency Priority Goal in the President's Management Agenda.[33]

Federal agencies can also lower the barriers to entry into the cybersecurity R&D marketplace by funding common research infrastructure (e.g., testbeds and datasets) to lower the cost of entry for small businesses, startup companies, and academic institutions, and to increase overall participation in R&D.

Expand diversity of expertise and diversity of workforce in cybersecurity.

Cybersecurity is more than technology. To accelerate progress, traditional cybersecurity research should be augmented with expertise from social, behavioral, and economic disciplines. Multidisciplinary research should be promoted by funding agencies and by research institutions. Agencies should ensure that grant solicitations encourage multidisciplinary proposals. Research institutions should ensure that personnel advancement (e.g., tenure) decisions value multidisciplinary research successes and publications as highly as traditional tenure criteria.

Diversity encompasses race, gender, ethnic group, age, personality, cognitive style, education, background, and more. Harnessing the talents of a workforce that includes people of all backgrounds who are diverse in thought, experience, and skills is essential to enabling innovation and creative discovery. Organizational leaders should take measures to foster an inclusive workplace climate in cybersecurity to attract and recruit new talent and maximize workforce engagement. Federal agencies should work with cybersecurity stakeholders to promote the visibility of cybersecurity careers and increase the mobility of cybersecurity professionals across government, industry, and academia.

[33] https://www.performance.gov/CAP/lab-to-market/

Abbreviations

5G	fifth-generation wireless networking technologies
AI	artificial intelligence
CPS	cyber-physical systems
DHS	Department of Homeland Security
HW	hardware
IoT	Internet of Things
IT	information technology
IWG	Interagency Working Group
K–12	kindergarten to 12th grade
ML	machine learning
NCO	National Coordination Office
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development (Program and NSTC Subcommittee)
NSF	National Science Foundation
NSTC	National Science and Technology Council
OSD	Office of the Secretary of Defense
QIS	Quantum Information Science
QKD	quantum key distribution
R&D	research and development
S&T	science and technology
SW	software
TDDI	trustworthy distributed digital infrastructure